Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

LUCAS C. FONTELA

ESTUDO DE CASO DE APLICAÇÃO DA POLÍTICA DE SEGURANÇA E SUA COMUNICAÇÃO PARA UMA EMPRESA

Brasília
2016

LUCAS C. FONTELA

ESTUDO DE CASO DE APLICAÇÃO DA POLÍTICA DE SEGURANÇA E SUA COMUNICAÇÃO PARA UMA EMPRESA

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu em Rede de Computadores com ênfase em Segurança da Informação.

Orientador: Prof. MA. Gilberto de Oliveira Netto

Brasília
2016

LUCAS C. FONTELA

ESTUDO DE CASO DE APLICAÇÃO DA POLÍTICA DE SEGURANÇA E SUA COMUNICAÇÃO PARA UMA EMPRESA

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Rede de Computadores com ênfase em Segurança da Informação.

Orientador: Prof. MA. Gilberto de Oliveira Netto

Brasília, 19 de outubro de 2016.

Banca Examinadora

_____

Prof. Dr. Nome completo

_____

Prof. Dr. Nome completo

Este trabalho dedico àqueles que acreditam na força de vontade, que acreditam que a vitória vem da sua persistência, dedicação e fé. Dedico a todos que amam a segurança da informação e a veem como grande investimento e não como despesa. Por fim, a minha família que me impulsionou a conquistar mais uma fase da minha carreira.

AGRADECIMENTOS

Sobretudo à Deus, meu criador e mantenedor da minha vida nessa terra. Todo louvor e glória a Ele. Seguidamente, a minha família que acompanha minha vida acontecer no outro cômodo da casa. Enquanto passo noites e dias trancado fazendo ciência, como diz uma antiga professora minha. E a minha futura esposa que espera ansiosamente a noite de sábado chegar para juntos sonharmos com o dia de amanhã enquanto aproveitamos a doce companhia do momento e o carinho apaixonante de um para com o outro.

Sem diretrizes a nação cai; o que a salva é ter muitos conselheiros. Provérbios 11:14 NVI

RESUMO

Este trabalho apresenta um estudo de caso em uma empresa de turismo em que seu objetivo é a implantação de uma política de segurança da informação e a execução de sua comunicação e treinamento em segurança da informação aos usuários da organização. Para isso se utilizou das normas técnicas da família ISO/IEC 27000 e conceitos de autores que descrevem sobre o tema. O processo de escrita dos regulamentos é diferente para cada organização e deverá ser elaborado conforme os seus objetivos de negócio. Comunicar esses regulamentos para os usuários da organização ao final do projeto é imprescindível para se obter um ambiente consciente de como a alta gestão deseja o tratamento da segurança dos ativos de informação da organização. Também foi realizado juntamente ao setor de comunicação dos regulamentos uma campanha de treinamento em segurança da informação divulgada por meio eletrônico e por palestras. Para obtermos a mensuração dos resultados alcançados por esta campanha e do nível de entendimento do assunto de segurança da informação dos colaboradores da organização disponibilizamos a eles dois questionários que foram distribuídos em fases diferentes dessa campanha. Na primeira fase, início da campanha, os resultados apontaram um deficit de conhecimento da política de segurança da organização quanto as questões básicas de segurança da informação. E na segunda fase, final da campanha, obteve-se um resultado positivo de quase 30% do nível de conhecimento deles quanto a política de segurança da organização e da segurança da informação.

Palavras-chave: Política de Segurança da Informação. Comunicação e treinamento. Segurança da informação. ISO/IEC 27000

ABSTRACT

This academic work presents an applied study case in a tour company which the main goal was the implantation of a security policy regarding the information itself, the execution of the communication and training focused in information's security for the organization's users. To achieve this purpose, it was used the technical standards of ISO/IEC 27000 category and notions of authors who stand up on the subject. The regulations' writing process is different for each organization and should be elaborated according to their business purpose. Report these regulations for the users' organization in the end of the project is essential to obtain a conscious environment of how about the high management want to deal with the security of the organization's information assets. Also was performed with the communication of regulations sector, a training campaign on information's security published electronically and by lecture. To get the mensuration of the achievements, by this campain, with the contributors' knowledge level on the subject, which is information security, we provide to them two questionaries, which was distributed in different moments of this campain. At the very first momento of the campain, the results showed a lack of knowledge about security policy of the organization, just like security information basics issues. At the second moment, in the end of the campain, it was obtained a positive increase of almost 30% of the knowledge level about politics and information security problems.

Key words: Information's Security Policy. Communication and training. Information's security. ISO / IEC 27000.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

BS - British Standard

CEOs - Chief Executive Officers

CFOs - Chief Financial Officers

CIOs - Chief Information Officers

DEPUB - Departamento De Publicidade

DITEC - Diretoria De Tecnologia

EAP - Estrutura Analítica de Projetos

GECOI - Gerência de Comunicação Interna

GEDEN - Gerência de Desenvolvimento

GEINF - Gerência de Infraestrutura

GESUP - Gerência de Suporte Tecnológico

IP - Protocolo De Internet

IEC - International Electrotechnical o Commission

ISO - International Organization for Standardization

LG - Luiz Guelman

MRMN - Módulo Risk Manager News

NBR - Norma Brasileira

NSA - National Security Agency

PCN - Plano de Continuidade do Negócio

PSI - Política de Segurança da Informação

PWC - Price Waterhouse Coopers

S.I. - Segurança Da Informação

SGSI - Sistema de Gestão da Segurança da Informação

SUMAP - Superintendência De Marketing E Publicidade

TI - Tecnologia da Informação

INTRODUÇÃO

As empresas de hoje que não enxergam a necessidade de manter seus perímetros seguros contra os ataques cibernéticos estão correndo grande perigo de serem alvos desses ataques. Esses ataques podem custar para as empresas percas financeiras mensuráveis quanto imensuráveis. CARBONE (2014, p.3) comenta que:

> De modo geral, os custos e a complexidade para responder aos incidentes estão aumentando. Isso inclui o custo de investigar; de entender os riscos de negócios e conter os incidentes; de gerenciar a notificação aos órgãos reguladores, clientes e consumidores; e de litígio. Além disso, o custo de remediação está crescendo porque mais registros em mais jurisdições estão sendo afetados, e os controles de segurança não estão acompanhando o ambiente de ameaças em constante mudança.

Há um alerta que podemos identificar se a questão de segurança de uma organização está sendo levada a sério, se a sua Política de Segurança está atualizada, se é praticada e se seus controles são eficientes ao seu negócio. Não somente isso, ela deverá andar acompanhada com um programa de conscientização e treinamento para os funcionários, tornando assim a segurança da informação mais eficiente a medida que os usuários entendem seu papel como agentes da segurança da informação. O ex hacker, Kevin Mitnick, que ficou conhecido mundialmente por suas façanhas e expertises comenta sobre Políticas de Segurança em seu livro, A arte de enganar, ele diz:

> As Políticas de Segurança são instruções claras que fornecem as orientações de comportamento do empregado para guardar as informações, e são um elemento fundamental no desenvolvimento de controles efetivos para contra-atacar as possíveis ameaças à segurança. Essas políticas estão entre as mais significativas no que diz respeito a evitar e detectar os ataques [...]
>
> Os controles efetivos de segurança são implementados pelo treinamento dos empregados, bem como por políticas e procedimentos bem documentados. Entretanto, é importante observar que as políticas de segurança, mesmo que sejam seguidas religiosamente por todos os empregados, não evitam todos os ataques da engenharia social. Por isso, um objetivo ideal seria sempre minimizar o risco até um nível aceitável. (MITNICK, 2003, p. 208).

Ele ressalta que é importantíssimo que uma empresa tenha o corpo de colaboradores treinados em segurança da informação, já que suas ações

exploravam sempre as deficiências de sistemas e a engenharia social, seu grande trunfo. MITNICK (2003, p 64) prossegue em seu argumento:

> De nada adianta ter uma estrutura forte se por dentro é fraca (ou macia), como uma concha. Conhecemos isso como segurança suave, ditado que foi criado por dois pesquisadores da Bell Labs, Steve Bellovin e Steven Cheswick.

Por tanto, não adiantará muito se a organização tiver na borda do seu perímetro de segurança uma proteção forte com um dispositivo bem configurado e por dentro desse perímetro os colaboradores forem descuidados ou desavisados da importância de seguir os protocolos de segurança da informação. Uma vez tendo acesso a uma informação valiosa, o atacante poderá muito bem acessar por meios legais os sistemas e tomar quaisquer ações danosas à empresa.

Não limitado à Política de Segurança, diversas outras ferramentas também terão de ser adotadas para evitar ou minimizar os danos de um ataque cibernético, como uso de equipamentos de filtros de pacotes, antivírus, etc, mas esse estudo se limitará a não tratar dessas questões, se atendo somente a Política de Segurança da Informação - PSI, e a sua comunicação.

A informação é um importante ativo de uma organização, por isso ela tem de ser protegida. Dependendo da classificação dessa informação, a exposição dela pode levar uma empresa ao fracasso, por exemplo, a exposição da fórmula da Coca-Cola ou dados de um governo, como no caso de Edward Snowden, que expôs casos de espionagem do governo americano quando trabalhava na NSA[1], em 2013.

Neste estudo de caso uma empresa de turismo foi vítima de ataque cibernético devido as brechas de segurança em sua política de segurança e a uma má implementação de códigos em seus sistemas. Com isso realizaremos a construção de uma nova Política de Segurança da Informação baseada na norma técnica ABNT NBR ISO/IEC 27002:2013 e criar um plano de comunicação e educação em segurança da informação aos usuários dessa organização a fim de reparar as vulnerabilidades existentes.

---

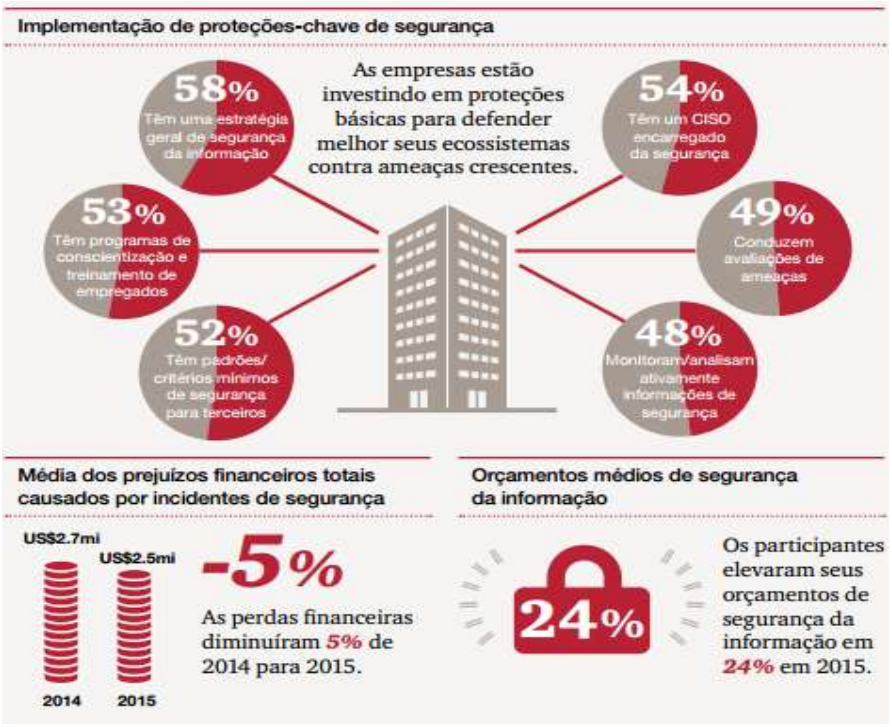
[1] NSA – National Security Agency. Agência de Segurança Nacional dos Estados Unidos da América. Site: https://www.nsa.gov/

Comumente sabe-se de empresas que tiveram seus sistemas invadidos através de brechas de segurança que poderiam ter sido evitadas se houvesse uma política de segurança implantada de maneira eficaz e eficiente. Algumas empresas criam as suas políticas, porém não se preocupam em cumpri-las. Criam motivadas a cumprir determinadas legislações e não em prover uma segurança eficiente aos ativos da organização. Por outro lado, outras empresas têm adotado sistemas inovadores de segurança e programas de conscientização para educar seus funcionários no intuito de reduzir os riscos de segurança cibernética, é o que diz a pesquisa da Price Waterhouse Coopers - PWC (2016, p. 1):

> Cada vez mais, elas (as empresas) adotam modelos e tecnologias inovadoras, como a segurança cibernética baseada na nuvem, Security Analytics e a autenticação avançada para reduzir riscos e melhorar seus programas de segurança.
>
> As organizações também estão adotando programas de conscientização para apoiar a educação dos empregados e executivos sobre os fundamentos da segurança cibernética, bem como sobre as vulnerabilidades que atacantes podem explorar envolvendo pessoas.

Ela ainda apresenta uma pesquisa logo em seguida, a Pesquisa Global de Segurança da Informação 2016, que foi realizada on-line nos meses de maio a junho de 2015 que contou com a participação de 10 mil pessoas, dentre elas Chief Executive Officers - CEOs, Chief Financial Officers - CFOs, Chief Information Officers - CIOs, e diretores de Tecnologia da Informação - TI, entre outros. Diz também que houve um aumento nos investimentos de segurança da informação. PWC (2016, p. 1): “Segundo os entrevistados, outra medida notável de progresso é uma renovada vontade de investir em segurança: registramos um aumento de 24% no orçamento das empresas destinado a esse tema. ”, e que por coincidência ou não, houve uma queda de 5% nas percas financeiras por incidentes de segurança no período de 2014 para 2015. A figura 1, a baixo, demonstra a porcentagem de proteção-chave de segurança adotadas pelas empresas pesquisadas.

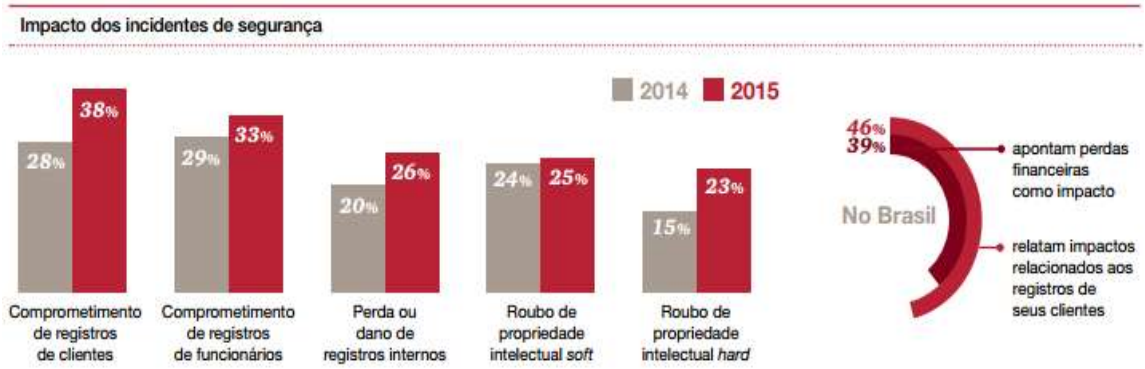
FIGURA 1 PROTEÇÃO-CHAVE DE SEGURANÇA



FONTE: PWC - 10MIN SEGURANÇA DA INFORMAÇÃO 2016

Ainda de acordo com essa pesquisa, as empresas aumentaram seus investimentos com segurança da informação no ano de 2015 mais que no ano de 2014. Sendo que as que mais investiram foram as pequenas empresas, já as grandes se mantiveram no mesmo patamar de investimentos. Segundo a PWC (2016), as organizações dizem que os principais alvos de ataques cibernéticos são as informações de funcionários e de clientes e que ainda o roubo de propriedade intelectual de uso estratégico subiu significativamente. A figura 2, demonstra esse percentual de incidentes de segurança.

FIGURA 2 INCIDENTES DE SEGURANÇA



FONTE: PWC - 10MIN SEGURANÇA DA INFORMAÇÃO 2016

O fato ocorrido com a empresa de turismo, Royal Magnífica, não foi diferente. Ela teve seu sistema invadido através de brechas em sua segurança que poderia ter sido evitadas com a utilização de controle de senhas descritos na norma de segurança da informação ISO/IEC 27002 e com a implementação de mecanismos de segurança em logon nos seus sistemas.

Portanto, este problema nos leva a duas indagações que direcionam essa pesquisa:

- Se a empresa dispusesse da sua PSI atualizada e seus controles elaborados fossem mais eficientes, este evento de segurança teria ocorrido?
- É importante a existência de campanhas educacionais que tratam especificamente da segurança da informação numa organização?

No entanto, este projeto de pesquisa tem como objetivo geral apresentar uma Política de Segurança da Informação como resposta ao incidente de segurança visando obter um ambiente empresarial mais seguro, sanando as brechas de segurança identificadas pela auditoria a pós a invasão em seus sistemas computacionais. Progredindo na sua capacidade de manter a confidencialidade, integridade e disponibilidade dos seus ativos e podendo oferecer maior confiança aos seus parceiros e clientes no trato de segurança da informação.

Para a realização desse objetivo, será necessário atualizar a atual PSI da empresa Royal Magnífica, colocando-a em conformidade com a versão mais recente

norma técnica de segurança da informação, ABNT NBR ISO/IEC 27002:2013, e também implementar e realizar uma campanha de educação em segurança da informação abordando as características de um ambiente seguro, papeis de cada usuário na segurança da informação, a divulgação da nova Política de Segurança da Informação atualizada e a instrução de alguns controles desta Política para os funcionários desta empresa.

Este trabalho se limitará aos objetivos de atualizar a PSI e realizar a sua comunicação e educação em segurança da informação. Questões como a elaboração e estruturação de um Sistema de Gestão da Segurança da Informação - SGSI, gestão de riscos, como foi realizada a análise de riscos por uma empresa terceirizada e softwares e hardwares especialistas não serão abordadas. Ficarão como ideias para estudos posteriores.

Espera-se demonstrar com este estudo de caso a importância da manutenção periódica da norma de segurança da informação numa organização e adequando-a as necessidades do seu negócio junto com as novas tecnologias existentes. Também a sua comunicação e o treinamento em segurança da informação aos usuários da organização que são estratégias fundamentais para manter um ambiente mais seguro aos ativos de informação de uma organização.

O presente trabalho foi então estruturado em 4 capítulos.

No primeiro capítulo, apresenta-se o referencial teórico que foi utilizado para este estudo, o segundo capítulo demonstra o estudo de caso na empresa; no terceiro capítulo, apresenta-se o processo de escrita da nova PSI; o quarto capítulo, demonstra o processo da criação e execução da campanha de educação e comunicação da PSI aos funcionários da organização.

1 REFERENCIAL TEÓRICO

Neste capítulo serão introduzidas as normas técnicas da família ISO/IEC 27000 que definem as normas de segurança da informação logo em seguida serão apresentadas as demais referências sobre política de segurança da informação e sua importância para uma organização. Serão abordadas as normas ISO/IEC 27000:2016 que apresenta o glossário de termos usados nas demais normas da família ISO/IEC 27000, a norma ISO/IEC 27001:2013 que define as estratégias de processo para estabelecer e implementar um Sistema de Gestão de Segurança da Informação – SGSI, de uma organização e a norma ISO/IEC 27002:2013 que faz a referência aos controles de segurança da informação e ajuda na construção da Política de Segurança da Informação.

As normas da família ISO/IEC 27000 são normas internacionais que tratam de modelos para sistema de gestão de segurança da informação (SGSI) a serem adotados e praticados por todo tipo e tamanho de organização. Elas são divididas por manuais de diferentes temas e passam por revisões periódicas. Atualmente a família conta com cerca de 20 manuais produzidos que levam em seu título geral *Tecnologia da Informação – Técnicas de segurança.* No Brasil elas são traduzidas pela Associação Brasileira de Normas Técnicas (ABNT) que é o Fórum Nacional de Normatização.

Quase todas normas de segurança da informação são originárias do Governo Britânico, é o que afirma FERNANDES (2012). A norma ISO/IC 27002 no início era conhecida pelo nome de BS 7799, BS que significava British Standard, que deu origem à ISO 17799 e posteriormente substituída pela ISO/IEC 27002 (a partir de 2007). Da mesma forma como ocorreu com a 17799, a BS 7799-2:2002 se transformou na ISO/IEC 27001.

A ISO (International Organization for Standardization) e IEC (International Electrotechnical o Commission) formam o sistema especializado para padronização mundial. Os organismos nacionais que são membros da ISO ou IEC participam do desenvolvimento de normas internacionais através comités técnicos estabelecidos

pela respectiva organização para lidar com campos particulares de atividades técnicas. Essa mesma informação poderá ser encontrada em todos os prefácios das normas da família ISO/IEC 27000.

1.1 ISO/IEC 27000:2016

A ISO/IEC 27000:2016 – *Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Visão geral e vocabulário*, é a norma que introduz a família de normas de gestão de segurança, nela é apresentado o glossário dos termos usados nas demais normas de sistemas de gerenciamento de segurança da informação, como nas ISO/IEC 27001, 27002, 27005, etc, que também as citam como referência de seus vocábulos. Ela apresenta sua definição em seu escopo, onde escreve:

> Esta Norma fornece a visão geral de sistemas de gestão de segurança da informação, e termos e definições comumente utilizadas na família de normas de SGSI. Esta norma é aplicável a todos os tipos e tamanhos de organizações (por exemplo, empresas comerciais, agências governamentais, organizações sem fins lucrativos). (ISO, 2016, p. 1).

Nesta parte serão referenciados somente os vocabulários utilizados para este trabalho pela norma de gerenciamento de segurança da informação ABNT NBR ISO/IEC 27002:2013.

Baseado nas definições descritas na norma ISO/IEC 27000:2016, capitulo dois, os termos e definições mais usados são descritos como:

- Controle de acesso – meios para assegurar que o acesso aos bens seja autorizado e limitados com base em requisitos de negócios e de segurança;
- Ataque – tentativa destruir, expor, alterar, inutilizar, roubar ou ganhar acesso não autorizado ou fazer uso não autorizado de um ativo;
- Auditar – processo sistemático, independente e documental para obter evidência de auditoria e avaliá-la objetivamente para determinar a extensão em que são cumpridos os critérios de auditoria;

- Autenticação – prestação de garantia de que uma característica de reivindicado de uma entidade é correta;
- Autenticidade – propriedade de que uma entidade é o que afirma ser;
- Disponibilidade – propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada;
- Confidencialidade – propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
- Conformidade – cumprimento de um requisito;
- Consequência – resultado de um evento;
- Objetivo de controle – descrição do que deve ser alcançado como resultado de controles de implementações;
- Ação corretiva – ação para eliminar a causa de uma não conformidade e para prevenir a recorrência;
- Dados - coleção de valores atribuídos a medidas de base;
- Eficácia - medida em que as atividades planejadas são realizadas e os resultados planejados são alcançados;
- Evento – ocorrência ou mudança de um determinado conjunto de circunstâncias;
- Gerência executiva – pessoa ou grupo de pessoas que tem responsabilidade delegada para governar o órgão para a implementação de estratégias e políticas afim de cumprir os propósitos da organização. Muitas vezes chamada também de alta gestão;
- Segurança da informação – preservação da continuidade, integridade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repudio e confiabilidade, podem também estar envolvidas;

- Evento de segurança da informação – uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;
- Incidente de segurança da informação – um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;
- Integridade – propriedade de salvaguarda da exatidão e completeza de ativos;
- Política - intenção e direção de uma organização, como expressas formalmente pela alta gestão;
- Ameaça - potencial causa de um incidente indesejado, que pode resultar em danos a um sistema ou organização;
- Alta gestão (administração) - pessoa ou grupo de pessoas que dirige e controla uma organização ao mais alto nível;
- Validação - confirmação, através do fornecimento de evidência objetiva, de que os requisitos para um uso ou aplicação pretendida específicas foram cumpridas;
- Vulnerabilidade - fraqueza de um ativo ou de controlo, que pode ser explorado por uma ou mais ameaças.

1.2 ABNT NBR ISO/IEC 27001:2013

A norma ABNT ISO/IEC 27001:2013 - *Técnicas de Segurança da Informação - Sistema de gestão de segurança da informação - Requisitos*, define os requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação – SGSI, e também incluí os requisitos para a avaliação e tratamento dos riscos da informação em qualquer tipo e

tamanho de organização que deseja implementar um SGSI, pois seus os requisitos descritos são genéricos, adaptando-se a quaisquer natureza de organizações. A norma ISO/IEC 27001:2013 (2013a, p. 1) apresenta sua definição em seu escopo, onde escreve:

> Esta Norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da informação dentro do contexto da organização. Esta Norma também incluí requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização. Os requisitos definidos nesta Norma são genéricos e são pretendidos para serem aplicáveis a todas as organizações independentemente do tipo, tamanho ou natureza.

De acordo com FERNANDES (2012, p.412) a abordagem de processos para um SGSI é estabelecida para que os usuários foquem na importância de:

> Entender os requisitos de segurança da informação e a necessidade de estabelecer políticas e objetivos de segurança da informação. Implementar e operar controles para o gerenciar os riscos de segurança da informação de uma organização, no contexto dos riscos gerais da empresa. Monitorar e rever o desempenho e a eficácia do sistema de gestão de segurança da informação. Prover a melhoria contínua, com base em medição objetivas.

As organizações que desejam criar uma gestão de segurança da informação poderão contar com essa norma como direcionamento no seu processo de implantação. A ABNT (2013a) orienta que uma organização poderá adotar um SGSI e que isso faz parte da sua decisão estratégica. Também afirma que sua implementação é influenciada por diversos motivos, segunda a norma ABNT ISO/IEC 27001:2013(2013a, p. v), que diz:

> A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais, funcionários, tamanho e estrutura da organização.

O SGSI é estabelecido para garantir a implementação de controles de segurança, visando proteger os ativos, baseado nas premissas da avaliação de riscos. Segundo a ABNT (2013a, p. v) o SGSI “preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos” e consequentemente, continua dizendo que “fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados”. Ela ainda destaca que é importante a sua integração com os processos da organização onde diz:

> É importante que um SGSI seja parte e esteja integrado com os processos da organização e com a estrutura de administração global e que a segurança da informação seja considera no projeto dos processos, sistemas de informação e controles. (ABNT, 2013a, p. v).

Como parte da nova atualização desta norma, as referências dos vocabulários, termos e definições encontram-se na norma ISO/IEC 27000, *Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Visão geral e vocabulário*.

Esta norma determina seu escopo no capítulo 4.3 – *Determinando o escopo do sistema de gestão da segurança da informação*, onde diz que "A organização deve determinar os limites e a aplicabilidade do sistema de gestão da segurança da informação para estabelecer o seu escopo" ABNT (2013ª, p. 1). Ela ainda continua informando que para a determinação dos limites e aplicabilidade do SGSI a organização deve considerar as questões internas e externas, as partes interessadas e seus requisitos e as interfaces e dependências entre as atividades desempenhadas pela organização.

A estrutura da norma está disposta da seguinte forma:

a) Prefácio
b) 0 Introdução
    a. 0.1 Geral
    b. 0.2 Compatibilidade com outras normas e sistemas de gestão
c) 1 Escopo
d) 2 Referência normativa
e) 3 Termos e Definições
f) 4 Contexto da Organização
    a. 4.1 Entendendo a organização e seu contexto
    b. 4.2 Entendendo as necessidades e as expectativas das partes interessadas

c. 4.3 Determinando o escopo do sistema de gestão da segurança da informação

d. 4.4 Sistema de gestão da segurança da informação

g) 5 Liderança

a. 5.1 Liderança e comprometimento

b. 5.2 Política

c. 5.3 Autoridades, responsabilidades e papéis organizacionais

h) 6 Planejamento

a. 6.1 Ações para contemplar riscos e oportunidades

i. 6.1.1 Geral

ii. 6.1.2 Avaliação de Riscos de segurança da Informação

iii. 6.1.3 Tratamento de riscos de segurança da Informação

b. 6.2 Objetivo de segurança da informação e planejamento para alcançá-los

i) 7 Apoio

a. 7.1 Recursos

b. 7.2 Competência

c. 7.3 Conscientização

d. 7.4 Comunicação

e. 7.5 Informação documentada

i. 7.5.1 Geral

ii. 7.5.2 Criando e atualizando

iii. 7.5.3 Controle da informação documentada

j) 8 Operação
   a. 8.1 Planejamento operacional e controle
   b. 8.2 Avaliação de riscos de segurança da informação
   c. 8.3 Tratamento de riscos de segurança da informação

k) 9 Avaliação de desempenho
   a. 9.1 Monitoramento, medição, análise e avaliação
   b. 9.2 Auditoria Interna
   c. 9.3 Análise crítica pela Direção

l) 10 Melhoria
   a. 10.1 Não conformidade e ação corretiva
   b. 10.2 Melhoria Continua

m) Anexo A (normativo) - Referência aos controles e objetivos de controles

n) Bibliografia

No Anexo A - Referência aos controles e objetivos de controles, desta norma são apresentados controles derivados da norma ABNT NBR ISO/IEC 27002:2013, das seções 5 a 18 e devem ser usados em alinhamento com o item 6.1.3 - *Tratamento de riscos de segurança da Informação*.

1.3 ABNT NBR ISO/IEC 27002:2013

A norma ABNT NBR ISO/IEC 27002:2013 - *Técnicas de Segurança – Código de Prática para controles de segurança da informação*, define os controles de segurança da informação para que organizações de qualquer tipo e tamanho possam usar como referência tanto para uma implementação de sistema de gestão

de segurança da informação – SGSI, quanto para simplesmente implantarem controles de boas práticas.

Esta norma descreve seu objetivo da seguinte forma:

> Esta Norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização. (ABNT,2013b, p. 6).

Ela ainda prossegue dizendo que foi projetada para ser usada por organizações que pretendem “selecionar controles dentro do processo de implementação de um sistema de gestão de segurança da informação” e “implementar controles de segurança da informação comumente aceitos” e também “desenvolver seus próprios princípios de gestão da segurança da informação”.

Toda organização que deseje ou precise implementar um processo de segurança de suas informações poderá ter como base a utilização dessa norma. A versão anterior a esta ABNT NBR ISO/IEC 27002:2013, a ABNT NBR ISO/IEC 27002:2005 (2005, p. x) define o que é informação, ela diz “A informação é um ativo que, como qualquer um outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida”.

De acordo com a ABNT (2013b) a informação pode ser mantida, armazenada, coletada e processada em variados formatos, podendo ser em meio físico, eletrônico, e verbal. Define ainda o seu valor dizendo que a informação ultrapassa as palavras, números e imagens, e que ideias e marcas são exemplos de formas intangíveis da informação.

Sabendo da importância e do valor que tem uma informação, meios de segurança deverão ser adotados pela organização para que ameaças não se aproveitem das vulnerabilidades e de brechas para causar danos a organização. Diante isso a ABNT (2013b, p. 4) também define como a organização poderá alcançar a segurança da informação ao dizer:

> Uma segurança da informação eficaz reduz estes riscos, protegendo a organização das ameaças e vulnerabilidades e, assim, reduzindo o impacto aos seus ativos.

> A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização são atendidos.

A norma ABNT ISO/IEC 27001 - *Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos*, orienta os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação e também incluí os requisitos para a avaliação e tratamento dos riscos da informação. A ABNT ISO/IEC 27002 age em complemento a esta norma.

Esta norma também indica que controles poderão ser adotados de outras normas e que a organização não precisa necessariamente adotar todos os controles constantes na norma, e sim, aqueles controles que a organização julgar necessário ao tratamento de risco. Sobre isso ela comenta:

> A seleção de controles de segurança da informação depende das decisões da organização, baseadas nos critérios para aceitação de risco, nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado à organização, e convém que também esteja sujeito a todas as legislações e regulamentações nacionais e internacionais, relevantes. A seleção de controles também depende da maneira pela qual os controles interagem para prover uma proteção segura.
>
> Alguns dos controles nesta norma podem ser considerados como princípios básicos para a gestão da segurança da informação e podem ser aplicados na maioria das organizações. (ABNT, 2013b, p. 5).

Como parte da nova atualização desta norma, as referências dos vocabulários, termos e definições encontram-se na norma ABNT NBR ISO/IEC 27000 - *Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Visão geral e vocabulário*, que já foi mencionado em item anterior.

A norma ABNT NBR ISO/IEC 27002:2013 é estruturada por 14 seções de segurança da informação, 35 Objetivos de controles e 114 controles.

Logo a baixo será descrita a estrutura da norma.

a) 0 Introdução

a) 1 Escopo

b) 2 Referências normativas

c) 3 Termos e definições

d) 4 Estrutura desta Norma

e) 5 Políticas de segurança da informação

    a. 5.1 Orientação da direção para segurança da informação

f) 6 Organização da segurança da informação

    a. 6.1 Organização interna

    b. 6.2 Dispositivos móveis e trabalho remoto

g) 7 Segurança em recursos humanos

    a. 7.1 Antes da contratação

    b. 7.2 Durante a contratação

    c. 7.3 Encerramento e mudança da contratação

h) 8 Gestão de ativos

    a. 8.1 Responsabilidade pelos ativos

    b. 8.2 Classificação da informação

    c. 8.3 Tratamento de mídias

i) 9 Controle de acesso

    a. 9.1 Requisitos do negócio para controle de acesso

    b. 9.2 Gerenciamento de acesso do usuário

    c. 9.3 Responsabilidades dos usuários

    d. 9.4 Controle de acesso ao sistema e à aplicação

j) 10 Criptografia

    a. 10.1 Controles criptográficos

k) 11 Segurança física e do ambiente

    a. 11.1 Áreas seguras

    b. 11.2 Equipamentos

l) 12 Segurança nas operações

    a. 12.1 Responsabilidades e procedimentos operacionais

    b. 12.2 Proteção contra códigos maliciosos

    c. 12.3 Cópias de segurança

    d. 12.4 Registros e monitoramento

    e. 12.5 Controle de software operacional

    f. 12.6 Gestão de vulnerabilidades técnicas

    g. 12.7 Considerações quanto à auditoria de sistemas de informação

m) 13 Segurança nas comunicações

    a. 13.1 Gerenciamento da segurança em redes

    b. 13.2 Transferência de informação

n) 14 Aquisição, desenvolvimento e manutenção de sistemas

    a. 14.1 Requisitos de segurança de sistemas de informação

    b. 14.2 Segurança em processos de desenvolvimento e de suporte

    c. 14.3 Dados para teste

o) 15 Relacionamento na cadeia de suprimento

a. 15.1 Segurança da informação na cadeia de suprimento.

b. 15.2 Gerenciamento da entrega do serviço do fornecedor

p) 16 Gestão de incidentes de segurança da informação

a. 16.1 Gestão de incidentes de segurança da informação e melhorias

q) 17 Aspectos da segurança da informação na gestão da continuidade do negócio

a. 17.1 Continuidade da segurança da informação

b. 17.2 Redundâncias

r) 18 Conformidade

a. 18.1 Conformidade com requisitos legais e contratuais

b. 18.2 Análise crítica da segurança da informação.

1.4 Política de Segurança da Informação

De acordo com BASTOS (2009), o objetivo da Política de Segurança da Informação é apresentar diretrizes e orientar a organização sobre a segurança da informação. Ele ainda aponta que os primeiros passos para a definição de um SGSI a PSI deverá ser definido formalmente e que essa política de segurança da informação deve refletir a visão da alta administração para um comprometimento do grupo executivo. Ainda de acordo com ele:

> A simples existência deste documento, que deve refletir a visão da alta administração frente à importância da informação, demonstra o comprometimento do grupo executivo com o plano estratégico de segurança da informação. (BASTOS, 2009, p; 61).

MARTINS (2003, p. 336) também comenta sobre a Política de Segurança em seu livro sobre gestão de projetos:

> A Política de Segurança é composta por um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações e serviços

> importantes para a empresa recebam a proteção conveniente, de modo a garantir a sua confidencialidade, integridade e disponibilidade.

Segundo FERREIRA (2006, p. 9):

> A Política de Segurança define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação.
>
> A política, preferencialmente, deve ser criada antes da ocorrência de problemas com a segurança, ou depois, para evitar reincidências.

A norma ABNT NBR ISO/IEC 27002:2013 orienta variados controles de segurança para serem implementados e seguidos. Ela própria define em seu primeiro controle que a política de segurança da informação deverá "prover uma orientação e apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. " (ABNT, 2013b, p. 8).

Cada organização deverá definir os controles e as restrições na sua implementação, tudo isso de acordo com os requisitos do negócio. Às vezes, a informação que é valiosa para uma organização não tem o mesmo valor para outra. Assim o projeto de implantação de uma PSI varia de tamanho, podendo ser médio ou grande, tudo isso depende da abrangência da política, da dispersão geográfica e do próprio tamanho do cliente, afirma MARTINS (2003).

De acordo com FONTES (2012), o recurso essencial para as organizações, tanto para as grandes quanto para as pequenas é a informação. Ela é um fator para o sucesso e para a continuidade da organização. A informação é capaz de aumentar as chances no mercado onde atua.

Para Domeneghetti e Meir (2009 apud FONTES, 2012, p. 4) "os bens ativos de uma organização podem ser classificados como bens intangíveis e bens tangíveis", ele continua dizendo que "os tangíveis são os bens físicos ou bens financeiros. Os bens intangíveis podem ser divididos em que geram valor e que protegem valor", logo em seguida eles citam exemplos de intangíveis que geram valor como "as Marcas, a Inovação e o Capital Intelectual" e os que protegem o valor como "a Segurança da Informação, a Gestão de Risco e a Governança Corporativa".

Para então continuar o processo de segurança da informação após ser concluída a construção da PSI ela deverá ser comunicada a todos usuários da

organização para a garantia de que a segurança e todo esforço para a sua construção não seja em vão. Diante isso, a norma ABNT ISO/IEC 27002:2013 que define sobre os controles de segurança também regulamenta sobre a conscientização, educação e treinamento em segurança da informação, ela informa que:

> Convém que o programa de conscientização considere um número de atividades de conscientização, tais como, campanhas (por exemplo, dia da segurança da informação) e a publicação de boletins ou folhetos. (ABNT, 2013b, p. 20)

FERREIRA (2006, p3) também comenta que:

> Entretanto, a garantia que uma organização possuíra um grau de segurança razoável está diretamente ligado nível de conscientização de seus colaboradores, ou seja, a segurança somente será eficaz se todos tiverem pleno conhecimento do que é esperado deles e de suas responsabilidades.
>
> Vale lembrar que a comunicação é um fator crítico de sucesso para a correta disseminação das políticas corporativas, já que esta provoca alterações no *status quo* de praticamente todos os colaboradores. Consequentemente obriga a mudanças na forma de trabalho e qualquer mudança gera resistência, sendo a comunicação a melhor maneira de reduzir os conflitos inerentes a ela.

SÊMOLA (2003, p. 136) afirma que “é fundamental que ela [PSI] seja reconhecida pelos funcionários como o manual de segurança da empresa”, ele ainda continua dizendo que as divulgações aos usuários poderão ser feitas por cartazes, peças promocionais, jogos, protetores de tela, e-mails, comunicados internos, etc. Ainda segundo ele:

> O nível de segurança de uma corrente é equivalente à resistência oferecida pelo elo mais fraco. O *peopleware* representa justamente esse elo; por isso, deve ser alvo de um programa continuo e dinâmico, capaz de manter os recursos humanos motivados a contribuir, conscientes de suas responsabilidades e preparados para agir diante de antigas e novas situações de risco. (SÊMOLA, 2003, p. 136).

FERREIRA (2006, p. 20) também comenta sobre a comunicação da PSI, ele afirma:

> Os funcionários deverão estar preparados para o assunto por meio de avisos (comunicação interna, e-mail, intranet), reuniões de conscientização, elaboração de material promocional, treinamento direcionado e peça teatral.
>
> Os funcionários que não participam dos programas de treinamento e conscientização, torna-se os elos mais fracos na corrente de segurança, colocando em risco todo o investimento.

O site Modulo (2006)[2], apresentou uma entrevista com o palestrante Luiz Guelman sobre “Conscientização de usuários: como envolver seu público com a Segurança da Informação”, para o evento CSO Meeting 2005. Nessa oportunidade, foram realizadas as seguintes questões:

> A) MRMN[3] - Qual a importância de campanhas de conscientização dentro de um plano corporativo de segurança da informação?
>
> *LG[4] - De nada adianta investir em tecnologia e proteção física se não temos a colaboração e o comprometimento das pessoas. Nas organizações, a grande maioria dos empregados tem uma falsa sensação de segurança, principalmente quando estão utilizando recursos de informática, pois sabem que existem profissionais dedicados e softwares de segurança atualizados e se sentem de alguma forma protegidos.*
>
> Há também a necessidade de se promover uma mudança na cultura da organização. Empresas que até bem pouco tempo atendiam um mercado cativo viram-se, do dia para noite, inseridas num contexto de alta competitividade e esqueceram de preparar seus colaboradores para essa nova realidade.
>
> B) MRMN - Uma dúvida comum que aflige os profissionais de Segurança da Informação é por onde começar uma campanha deste porte. Diante de sua experiência, o senhor poderia nos apontar os possíveis caminhos para implementação de uma campanha de conscientização? E qual a importância da participação de outras áreas, como Recursos Humanos (RH) e Comunicação?
>
> LG - *Para o planejamento, é importante fazer uso de dois recursos fundamentais: o registro de ocorrências e as pesquisas de conhecimento. O primeiro aponta as principais vulnerabilidades já exploradas pelos agentes ameaçadores, permitindo priorizar as ações e as áreas/locais que requerem atenção especial. O segundo permite identificar as principais deficiências de conhecimento e de comportamento.*
>
> *O setor de RH deverá auxiliar na administração dos eventos, acompanhar a participação dos empregados e emitir os certificados de treinamento. Já a área de comunicação empresarial deve cuidar da confecção dos cartazes, "banners", brindes e comunicados, pois é a área que tem maior sensibilidade para a modalidade de campanha que o tema requer.*
>
> C) MRMN - Quais formas podem tornar uma campanha de conscientização atrativa para os colaboradores de uma empresa (uso de jogos, divulgação pela intranet, palestras, premiação etc)?
>
> *LG - As enquetes divulgadas através da intranet e os questionários utilizados nas pesquisas de comportamento são um passo importante para despertar a curiosidade dos colaboradores. É recomendável programar*

[2] Modulo, http://www.modulo.com.br/comunidade/entrevistas/616-conscientizacao-de-usuarios-como-envolver-seu-publico-com-a-seguranca-da-informacao

[3] MRMN, Módulo Risk Manager News.

[4] LG, Luiz Guelman.

> *ciclos periódicos dos eventos de divulgação que, dependendo do porte da empresa, poderão ter frequência semestral ou anual. Em cada ciclo deve ser escolhido um tema específico para ser trabalhado, conforme a prioridade requerida. A participação dos colaboradores nas apresentações deve ser espontânea e, para garantir uma boa adesão, é fundamental a divulgação dos eventos através de cartazes, banners e e-mails.*
>
> É necessária, também, muita criatividade para despertar o interesse do empregado. Palestras com temas que, além de atenderem às necessidades da empresa, possam servir para agregar valor às vidas pessoais de seus empregados, tais como vírus, uso de senhas, engenharia social e uso seguro do correio eletrônico são bastante eficazes. O uso de recursos lúdicos, tais como jogos educativos e peças de teatro, ajudam a fixar os conhecimentos.
>
> *Os ciclos seguintes de eventos devem ser repetidos nos locais onde já ocorreram, pois, os empregados que participaram dos eventos anteriores, e se sensibilizaram para o assunto, retornarão para reciclagem de seus conhecimentos e, com certeza os recomendarão para outros colegas.*
>
> *Os gerentes também desempenham um papel importante pois são eles que, já conscientizados, irão contribuir para o sucesso do evento, recomendando a participação de pessoas chaves da sua área.*

FONTES (2005), também apresenta um questionário sobre a importância da conscientização dos usuários da organização. Ele faz a indagação do por que a pessoa faz a diferença, e em seguida apresenta uma série de respostas com suas explicações, como:

> A) Porque as pessoas pensam em proteger apenas o computador.
>
> Jogar papel com informação confidencial no lixo sem destruir; deixar informação em salas após as reuniões, comentar informações confidenciais em lugares sem garantia de sigilo como elevador, táxi, avião e recepções de happy hour (onde os concorrentes estão) são procedimentos que as pessoas fazem sem querer, sem má fé, mas que podem prejudicar os negócios da empresa.
>
> B) Porque as pessoas que querem fraudar a organização vão mirar nas pessoas da organização.
>
> Aproveitando o descuido e a boa-fé das pessoas da organização, os malfeitores agem sobre essas pessoas, independentemente do nível hierárquico e da condição de conhecimento técnico. Todos são alvos dos que querem fraudar ou roubar informação da organização.
>
> C) Porque são as pessoas quem cumprem os regulamentos.
>
> Os regulamentos como políticas e normas são pano de fundo para o processo de segurança da informação. Eles cristalizam como a organização deseja que a proteção aconteça. Porém, para acontecer é necessário que os usuários leiam, entendam e executem esses regulamentos.
>
> D) Porque são as pessoas que não cumprem os regulamentos.
>
> Muitas vezes uma bela arquitetura e um conjunto de regras não alcançam sucesso pelo simples fato das pessoas não seguirem os regulamentos.

> E) Porque são as pessoas que passam para as outras pessoas os conceitos de segurança.
>
> Um funcionário novo vai receber da área de recursos humanos uma grande quantidade de papel contendo regulamentos e outras obrigações. Isso ajuda ele conhecer a organização. Mas, saber realmente como todos se comportam e consideram as regras, é pelo exemplo do colega, pelas ações da chefia e principalmente pela coerência da direção executiva.

Por fim, ainda sobre a comunicação da Política de Segurança, MITNICK (2003, p. 200) comenta que “Os melhores programas de treinamento sobre a segurança das informações devem informar e prender a atenção e o entusiasmo dos aprendizes”.

2 ESTUDO DE CASO

Este estudo foi elaborado em uma empresa de nome Royal Magnífica, que atua no setor de turismo e que tem seus serviços disponibilizados em ambiente físico (lojas) e ambiente web (site público). Nela foi relatada um evento de segurança em que foi vítima de invasão em seu site através de uma vulnerabilidade de segurança no logon de seu sistema. A existência desta brecha no sistema é decorrente a má implementação de controles de segurança e falha no desenho do sistema.

Não diferente disso, a sua política de segurança estava mal elaborada e não havia um programa de instruções em boas práticas de segurança, treinamentos e a comunicação da Política de Segurança da Informação - PSI, aos seus usuários, esses que são o elo mais fraco da corrente da segurança da informação.

Essa situação pode ser realidade de muitas empresas que não tem a preocupação em manter atualizada a sua Política de Segurança da Informação, e muito menos criam controles eficientes em seus sistemas. Muitas empresas deixam de implementar uma PSI eficiente porque ela poderá confrontar a cultura da empresa (que é o caso da empresa analisada) gerando assim um mal-estar com seus usuários, ou acham que seu perímetro de segurança já está bastante seguro ou ainda por a equipe técnica não ter o conhecimento suficiente das normas de segurança, especificamente da família ISO/IEC 27000, que tratam das Políticas e Normas de Segurança da Informação, que estipulam os controles para a segurança da informação.

O objetivo principal desse trabalho é demonstrar a aplicação de uma Política de Segurança da Informação e a implementação de uma campanha de educação e conscientização em segurança da informação aos colaboradores desta empresa para se estabelecer o ambiente mais sólido e seguro quanto as questões de segurança da informação.

2.1 Descoberta do problema

A empresa, Royal Magnífica, em análise de seu balanço semestral financeiro, identificou divergências em sua receita. Descobrindo que houve mais despesas em custos de operações com parceiros do que a arrecadação de seus serviços prestados a clientes. Sabendo que os valores de taxas com os parceiros não foram alterados a gerência de auditoria solicitou a alta direção para que autorizasse a instauração do processo de auditoria interna para a verificação da divergência na receita.

O processo de auditoria foi autorizado e envolveram as gerências de cadastro e reservas, gerência de vendas, gerência de auditoria e as gerências de tecnologia (no âmbito de desenvolvimento e de redes) para a coleta de informações necessárias. A elaboração e o processo de auditoria não serão abordados por este trabalho. Somente compartilharei o resultado final obtido por ela.

Indo direto ao resultado apontado pela auditoria, o deficit em sua receita veio de invasões aos seus sistemas de banco de dados através de seu site público. O atacante se aproveitou de uma brecha de segurança constante no site, onde o logon para acesso interno não era submetido a tratamento de bloqueio de conta de usuário após atingir um limite de tentativas frustradas. Observado os logs de acesso do sistema verificou-se que existiam diversos registros deste login com a indicação de erro na validação de logon por ser a senha diferente da correta. De acordo com o resultado destes logs suspeitamos que foi utilizado o método de ataque de força bruta no sistema pelo atacante até o êxito em sua ação. Posteriormente passando a acessar alguns sistemas internos com o login de um funcionário válido da empresa.

O atacante conseguiu alterar o cadastro de alguns ex-clientes, passando a situação deles de inativos para ativos e colocando em seu histórico financeiro como adimplentes. Foram marcadas várias hospedagens em hotéis parceiros e voos nacionais e internacionais para variados destinos. Esta ação durou cerca de oito meses até a data de descoberta.

Segundo a auditoria ainda, esses dados foram obtidos pelo confronto de informações com outro sistema de cadastro de ex-clientes do período semestral

onde não batiam as datas de ativação e nem os nomes de clientes que solicitaram a reativação da conta. Descoberto também que a conta de logon que foi utilizada no sistema foi encontrada pelos logs de acesso que foram sempre em horários diferente do comercial e os IPs diferentes da sua localidade padrão.

A invasão mostrou que existia uma brecha de segurança no tratamento de validação de logon e a falta de cuidado em se ter senhas fortes, situação que poderia também estar presente em outros sistemas da organização. A política de segurança em uso pela empresa descrevia sobre o tratamento de senhas, porém, suas diretrizes não eram totalmente implementadas nos sistemas da empresa o que facilitava a criação de senhas fracas pelos usuários e que dificultava a exigência de um padrão mais rigoroso para validação em sistemas computacionais da organização. As diretrizes de tipos de caracteres a serem usados em senhas, prazo de validade, bloqueio de conta por tentativas frustradas existiam apenas no papel, isso faz a PSI perder a credibilidade com os usuários, já que não era executado. É melhor não se ter um controle escrito do que escrito e não praticado.

Por exemplo, o sistema de serviço de diretório, Active Directory, não estava configurado para a exigência de tipos variados de caracteres na criação da senha (apesar de conter diretrizes para isso na antiga política), e não executava o bloqueio da conta após tentativas frustradas de logon, além de que existiam contas de usuários com a opção de senha nunca expirar ativadas, o que põe em risco a segurança das informações de variadas classificações no ambiente de rede da organização. Outro exemplo, um sistema de reservas em hotéis também apresentava vulnerabilidade na sua verificação da senha, onde também não existia o bloqueio da conta por tentativas de acesso frustradas.

Outro ponto a ser destacado é a cultura dos usuários da organização em relação as questões de segurança da informação que corroborava para o ambiente pouco seguro. Práticas como o uso indiscriminado do *pen drive* (favorecendo a infecção descontrolada nas estações de trabalho), o não bloqueio de tela ao se ausentar das estações, as conversas em corredores com informações críticas sendo divulgadas e a insatisfação em não poder repetir as suas últimas sete senhas utilizadas, achando penoso o trabalho de recriar uma nova senha de acesso a rede toda vez que solicitado pelo sistema de Active Directory.

Esses fatos demonstram a necessidade de uma Política de Segurança da Informação com controles mais eficientes e com seu verdadeiro cumprimento pela organização e também junto com a obrigação da mudança de hábitos dos usuários e da cultura existente na organização. A realidade da situação que se encontrava a empresa antes do evento de segurança tomou força no viés executivo e na alta gestão de modo que ela comprou a ideia do projeto dando todo apoio necessário à sua conclusão. Portanto, era o momento de se tomar novas atitudes para combater as ameaças de segurança, conforme diz a então diretora da PWC, OLIVEIRA (2014, p. 4):

> Não é possível combater as ameaças de hoje com as estratégias de ontem. É necessário um novo modelo de segurança da informação, que leve em consideração o conhecimento das ameaças do ciberespaço, dos ativos de informação e dos motivos e alvos dos potenciais atacantes.

A partir daí a Gerência de Infraestrutura - GEINF, se propôs a desenvolver e aplicar uma nova Política de Segurança da Informação e seu programa de comunicação e treinamento em segurança da informação aos colaboradores da empresa para que eles tomem ciência da proteção dos ativos e dos riscos de segurança existentes. De modo também que esse projeto servirá para a consolidação da nova maneira de combate as ameaças da organização.

2.2 A empresa

A Royal Magnífica é uma empresa de viagens e turismo, sediada em Brasília e atuante em todo o mercado nacional, possui diversas filiais por quase todos estados brasileiros. Seus produtos principais são: vendas de passagens áreas, hospedagem em hotéis, pacotes de viagens e títulos de hospedagem. É uma empresa de médio porte, com cerca de mil e duzentos colaboradores com a maioria deles lotados em sua sede.

O seu organograma é composto pela presidência, gerência de auditoria, gerência jurídica, diretoria de finanças, diretoria administrativa, e a diretoria de tecnologia. A baixo da diretoria de tecnologia – DITEC, existem as gerências de infraestrutura - GEINF, de suporte tecnológico - GESUP e a gerencia de desenvolvimento - GEDEN. A empresa ainda não dispõe de uma gerência específica

para tratar de assuntos referentes a segurança da informação. Essas questões são tratadas comumente pelas gerências de infraestrutura e de desenvolvimento. Na etapa seguinte, descreveremos como ocorreu o processo de escrita da Política de Segurança.

3 PROCESSO DE ESCRITA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Neste capítulo será descrito o processo de escrita da nova Política de Segurança da Informação, abordando as etapas de análise dos controles necessários, a definição da sua estrutura e a construção dos controles.

Após o evento de segurança, toda a GEINF foi reunida pelo seu gestor que alertou sobre a ocorrência do evento e comunicou sobre o novo projeto que nos envolveria. Nesta ocasião também foi definido o Grupo de Construção das Políticas e Normas de Segurança da Informação que participaria do processo de desenvolvimento deste projeto que contempla as partes de atualização da Política de Segurança da Informação descrevendo-a no padrão da norma ABNT ISO/IEC 27002:2013, desenvolver um plano de comunicação desta norma e um plano de conscientização das melhores práticas em segurança da informação aos funcionários da organização.

No início do estudo foi primeiramente feita uma análise da política de segurança vigente. Nesse processo foram examinados os controles e diretrizes da política, removido os controles que não faziam mais parte do objetivo do negócio da organização, separado os que precisavam ser atualizados e os que estavam de acordo. Também foram levantadas necessidades para os controles com as ocorrências diárias registradas no sistema de chamados interno, caso de uso de ativos (celulares e *tablets*), solicitação de serviços específicos categorizados para gestores, restrição de acessos rede/internet, entre outros que ajudaram na elaboração e definição dos novos controles, além de serem comparadas com os cumprimentos da norma. Foi também usado os controles levantados pela análise de riscos de uma empresa terceirizada que fora contratada para este serviço específico.

Em seguida, após a análise das necessidades, entrevistas foram realizadas com os gestores do jurídico, de recursos humanos e da alta gestão para o mapeamento claro dos controles de segurança a serem implementados de modo que estejam coerentes com os objetivos da organização e com regulamentos

jurídicos. No anexo B, deste estudo de caso, se encontra disponibilizada a antiga PSI que poderá ser verificada pelo leitor.

Alguns dos resultados levantados pelo Grupo de Construção das Políticas e Normas de Segurança da Informação da análise da antiga PSI estão descritos a seguir:

- Controles que apresentavam diretrizes escassas e algumas com o nível de detalhamento pertencente ao documento de normas e procedimentos. Como por exemplo:
    - Controle de senhas, que citado anteriormente regulamentava o tempo de expiração da senha em 90 dias (tempo muito longo - o uso de um tempo curto diminui a janela tempo de ação de um atacante na tentativa de sua descoberta), caracteres alfanuméricos (é recomendável o uso de símbolos e frases para dificultar o ataque de dicionário.
    - Controle de acesso remoto definia diretrizes de referente a outro controle de segurança.
    - Controle de uso de e-mail continha diretriz que especificava detalhadamente a ferramenta de correio eletrônico (esta informação deveria ser detalhada no documento de normas).
    - O controle do uso da internet e intranet se encontra no mesmo caso do citado anteriormente.
- Falta de atualização de documento:
    - Encontrado nome e sigla de gerência em desuso. Caso da SUMAP - superintendência de marketing e publicidade, que passará a ser DEPUB - departamento de publicidade.
    - Sem menção no texto do período a ser revisado o documento pelo setor responsável da empresa.
    - Ausência da assinatura de aprovação da alta gestão e a informação da data de entrada em vigor.

Entendemos que os resultados obtidos pelas análises realizadas demonstram que as diretrizes e controles poderiam ter sido implementados e cumpridos, evitando a invasão aos sistemas pela forma ocorrida e a falta de maturidade no tratamento do documento de política de segurança da informação. Uma Política clara e bem definida ajuda a segurança da empresa e fortalece a moral da equipe de tecnologia.

A etapa seguinte, após a entrega do resultado da análise anterior ao gestor da GEINF, contempla as próximas ações tomadas para escrita da nova PSI. De maneira que tomamos embasamento na norma técnica ABNT ISO/IEC 27002:2013 que já a descrevemos na seção de referencial teórico.

A construção faz uso das anotações das análises das necessidades (que também engloba a análise de riscos), seleção dos novos controles retirados da norma técnica alinhada aos objetivos e negócio da organização e com a participação da direção e dos gestores de diversas áreas da organização.

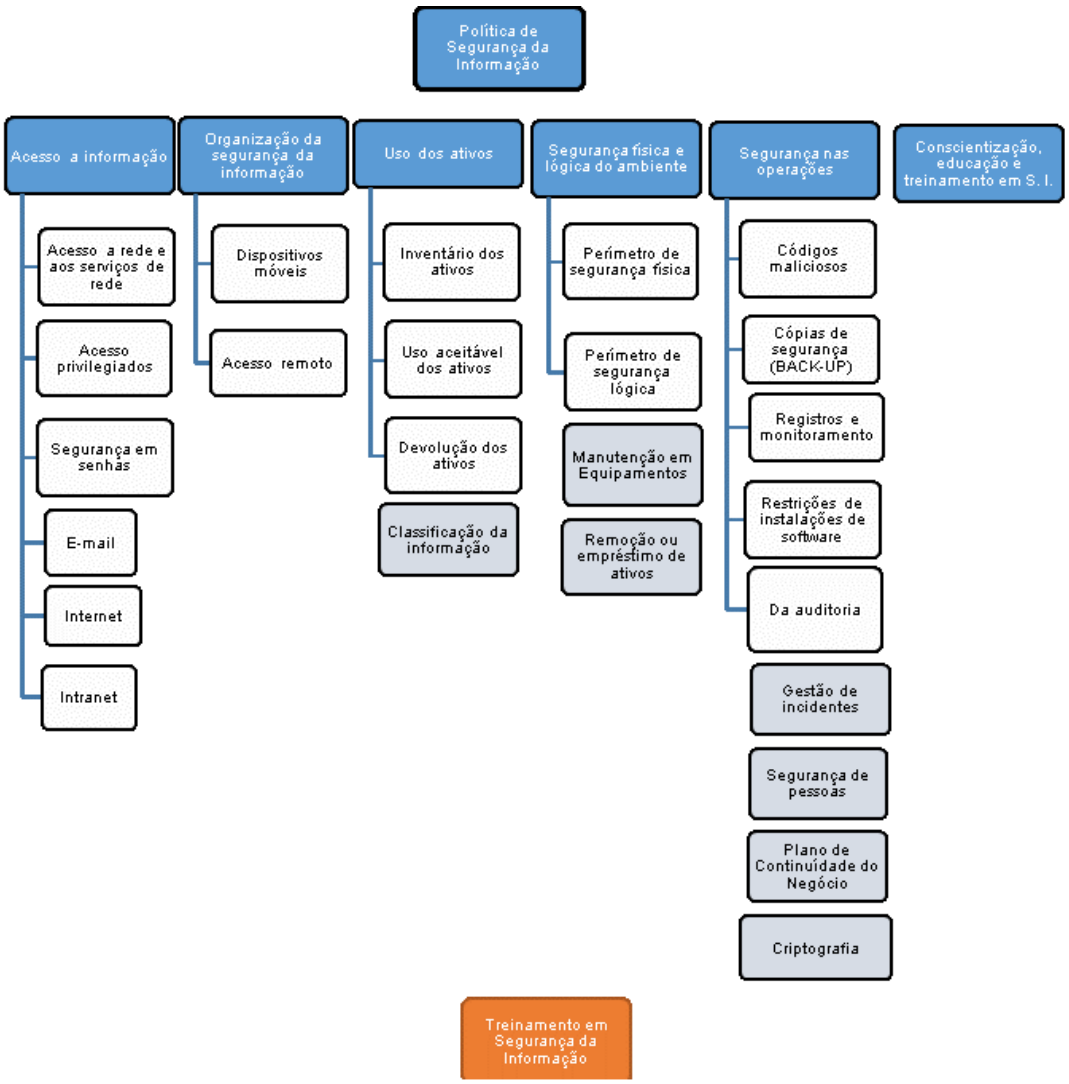
Como não existe uma arquitetura rígida para a estruturação dos regulamentos de uma PSI, decidimos por estruturá-la de maneira que facilite a separação dos seus regulamentos e do entendimento pelo leitor. A forma adotada segue conforme a de várias empresas e de órgãos públicos que utilizam para escrever a sua PSI. A escrevemos na forma de Política e Norma, separando os regulamentos por seu nível de granularidade.

Os regulamentos descritos em Política são diretrizes de orientações básicas que indicam o que se quer. Nele se tem a preocupação de não definir a maneira como deve ser feita nem a sua implantação. Deverá conter a assinatura pelo Presidente da organização ou que seja aprovada pelo conselho de administração da organização.

Em Norma, os regulamentos contêm as regras básicas de como deve ser implementado o controle ou o seu conjunto de controles que foram anteriormente definidos pela política da organização ou por outro regulamento que a organização deve seguir em conformidade.

Para a melhor ilustração da arquitetura da Política e Norma que desenvolvemos nesse trabalho, disponibilizamos a sua arquitetura na figura logo a seguir. Nela está descrito o que foi implantado e o que ainda está em fase de implementação (balões na cor de fundo azul mais claro). Com a criação da Arquitetura de Regulamentos para a Segurança da Informação a organização conseguirá ter uma correta visão da sua situação de maturidade e a extensão das normas e políticas de segurança da informação.

FIGURA 3 ARQUITETURA DE REGULAMENTOS PARA SEGURANÇA DA INFORMAÇÃO



FONTE – ADAPTADO DO LIVRO POLÍTICAS E NORMAS PARA A SEGURANÇA DA INFORMAÇÃO. BRASPORT, 2012

Definido a estrutura da nova PSI, passamos para o processo de criação dos seus regulamentos. De acordo com FONTES (2012, p. 82) em seu livro sobre Políticas e Normas para a Segurança da Informação cita que:

> Os regulamentos de segurança da informação são específicos para cada organização. Existem conceitos e controles que devem ser considerados por todas organizações, porém, a forma de implantação, a rigidez dos controles, a abrangência do público que será atingido e a granularidade das regras são específicos de cada organização. A política de segurança da informação deve ser uma consequência de como a organização deseja proteger a sua informação.

O autor continua dizendo que a organização precisa identificar a real motivação para a existência da Política de Segurança da Informação para implementar adequadamente os regulamentos. Ele, Fontes (2012), cita 5 razões pelas quais as empresas começam o processo de implantação sendo eles a “Legislação”, “Exigência do mercado e/ou dos clientes”, ” Adequação às melhores práticas”, “Avanço tecnológico” e “Necessidade do negócio”, nesta última onde se encaixa a empresa Royal Magnífica.

Os regulamentos que comporão a nova PSI começaram a serem escritos pelo Grupo de Construção e em seu processo foram feitos encontros com os gestores do jurídico, dos recursos humanos, suporte tecnológico, desenvolvimento, administrativo e da telefonia para o mapeamento dos controles de segurança, a fim de conhecer melhor as necessidades e o trabalho com a informação de cada setor. Os encontros com gestores das áreas foram importantes para que houvesse a implementação de controles e diretrizes coerentes com as necessidades da organização.

A construção dos controles depende do alinhamento aos objetivos da organização. Na ação que a empresa precisa determinar o nível de segurança que a informação terá, cabe ao Gestor da Segurança da Informação levantar essas informações. Ele é o encarregado de fazer os questionamentos, recomendar os controles e levantar os riscos. O Gestor da Informação deve ser da área de negócio e cabe a ele definir o grau de rigor nos controles que serão tomados.

A definição das políticas e normas de segurança no alinhamento com os gestores da informação seguem a prerrogativa de primeiro: saber o que é mais importante para os objetivos de negócio da organização. Depois definir quais serão

os seus requisitos de segurança e por fim o desenvolvimento das políticas e/ou normas.

Numa das entrevistas com a gerente de recursos humanos foi levantado o caso no controle de uso de e-mail corporativo que existem duas gerencias na empresa que não fazem uso do serviço de comunicação externa, então, a escrita deste controle deverá incluir essa exceção. Na entrevista com a gerencia jurídica foi verificado que sobre os regulamentos escritos se em sua forma e em seus controles poderiam apresentar algum risco jurídico para a empresa (ou seja, se não infringiria alguma lei).

Seguinte às entrevistas, o processo de escrita da norma adotou-se como referência o modelo de padrão mínimo de controles para a construção de uma PSI definido por Edison Fontes em seu livro sobre Políticas e Normas para a segurança. Em sua pesquisa, ele apresenta um estudo de caso realizado em dez organizações de grande porte e que possuem um patamar de maturidade de segurança da informação reconhecida no mercado. Na pesquisa ele elabora um conjunto de controles da ABNT NBR ISO/IEC 27002 que são comuns entre essas empresas e sugere como padrão mínimo de regulamentos que deverão existir na Política de Segurança de uma empresa. Ele diz:

> Um padrão mínimo de controles para uma política de segurança da informação, baseada no fato de que 30% dos controles da norma (NBR ISO/IEC 27002:2005) são utilizados por 70% das organizações. Este padrão mínimo é um excelente patamar inicial de controles de segurança e facilita a organização que está começando seu processo de segurança da informação. (FONTES, 2012, p. 81).

Esse conjunto de controles estabelecidos na pesquisa de FONTES (2012), a partir da página 250 são descritos como:

- Controle de acesso a informação;
- Gestão de ativos: Internet, equipamentos inteligentes, e-mail e outros;
- Classificação da informação;
- Cópias de segurança;
- Monitoramento do uso de sistemas;

- Política de segurança da informação;
- Conscientização, educação e treinamento;
- Encerramento de atividades: corte de acesso à informação;
- Trabalho remoto;
- Aquisição, desenvolvimento e manutenção de sistemas;
- Processo disciplinar;

Com base nessa pesquisa conseguimos observar o mínimo aceitável para a construção da nova política para a Royal Magnífica, porém, não será limitado a estes controles descrito por ele. Sabendo que a segurança da informação deve refletir o desejo da proteção que a empresa deseja para seu negócio, outros pontos de controles foram adicionados no intuito de ampliar a segurança da informação na organização. Regulamentos tais como uso dos ativos, dispositivos móveis, manutenção em equipamentos, remoção ou empréstimos de ativos, conscientização em segurança da informação, etc, não existiam anteriormente, mas agora fazem parte dessa atualização de forma a alcançar os requisitos de negócio da organização. Outros controles importantes também farão parte dessa nova organização da segurança como é o caso da segurança lógica, gestão de incidentes, segurança de pessoas, criptografia e plano de continuidade do negócio que antes não era mencionado e nem haviam processos para isso. Porém estes ainda estão em faze de implantação.

A linguagem a ser empregada na escrita do documento de Política de Segurança da Informação deverá ter o cuidado de não ser muito técnica e não conter termos complicados ao entendimento do leitor, deve ser uma linguagem simples, que o aproxime ao entendimento das orientações requeridas. Nessa política foi tido o cuidado de usar uma linguagem simples de maneira que facilite a comunicação entre o documento e aquele que o lê.

A PSI de alto nível da empresa Royal Magnífica foi estruturada na forma de Objetivo, Escopo, Definições, Atribuições, Regulamentos, Conclusão e Vigência. Onde o Objetivo diz o que é o documento, o que ele define e o que a organização

deseja comunicar com ele. O Escopo diz quais são os tipos de usuários que serão afetados pela norma. A Definição explica os termos técnicos utilizados no documento. As Atribuições definem as responsabilidades referentes ao documento, quem é o responsável pela atualização, pela divulgação, etc. Os Regulamentos contém as regras e orientações que a organização deseja que seus usuários obedeçam. Em Conclusão se encontra o resumo do comportamento aceitável, as penalidades pelo não cumprimento dos regulamentos e onde o usuário poderá buscar informações em caso de alguma dúvida. E em Vigência se encontra a data que o documento entra em vigor e a assinatura da alta gestão aprovando o documento.

No documento de Normas e Diretrizes, a estrutura obedece à forma de Objetivo e Regulamentos. Onde temos em Objetivo o resumo do que se trata a norma e em Regulamentos definição das diretrizes e orientações que a empresa deseja ser obedecida.

Ao ser findada as entrevistas e a política de segurança concluída e devidamente assinada pela alta direção, uma parte do controle de senhas comentado que foi citado anteriormente será demonstrado logo abaixo. Não estão descritas todas as diretrizes, somente algumas que sofreram alterações.

- PSI ANTIGA - Cada usuário é responsável pela utilização das senhas corporativas necessárias ao desempenho de suas funções.
- PSI ANTIGA - A senha é de uso pessoal e intransferível, sendo proibido o seu compartilhamento. Caso isso ocorra, é de total responsabilidade do usuário proceder à sua alteração.
    - COMENTÁRIO: Estas diretrizes foram reformuladas para uma escrita mais abrangente, especificando nela a guarda, sigilo e a proteção da senha como responsabilidade de cada usuário. E dividido os temas entre confidencialidade e alteração de senha.
    - PSI NOVA. Diretriz: *A guarda, sigilo e proteção da senha é de responsabilidade total do seu proprietário. Ela é pessoal e*

intransferível, a quebra da sua confidencialidade poderá incorrer em medidas administrativas;

- PSI NOVA. Diretriz: *Deverá ser alterada a senha sempre que houver suspeita de quebra de confidencialidade;*

- PSI ANTIGA - A senha de acesso deve conter, no mínimo, sete caracteres alfanuméricos (números e letras), sendo o usuário obrigado a escolher uma nova senha no momento do primeiro acesso.
    - COMENTÁRIO: Nessa diretriz foi incluído a obrigatoriedade da utilização de símbolos no conteúdo da senha para obtenção de uma maior segurança e também a dividida numa outra diretriz sobre a obrigatoriedade da troca da senha no primeiro logon do usuário para acesso à rede e sua exceção para aqueles que estão localizados nas filiais da empresa.
    - PSI NOVA. Diretriz: *A senha de acesso a rede da empresa Royal Magnífica deverá possuir o tamanho mínimo de 7 caracteres e ser utilizado caracteres alfanuméricos e símbolos;*
    - PSI NOVA. Diretriz: *É obrigatória a troca da senha no primeiro logon na rede, exceto casos de usuários em locais sem domínio de rede;*
- PSI ANTIGA - Não é permitido o uso de senhas óbvias, como datas, nomes próprios e siglas. Ela deve ser memorizada e nunca anotada em lugar de fácil acesso aos outros usuários.
    - COMENTÁRIO: Na produção dessa diretriz foi modificado o seu texto e dividida em duas diretrizes. Na primeira diretriz, definido sobre o que não poderá conter na formação da senha para dificultar o ataque de dicionário. Na segunda diretriz, descrito sobre a política de Tela Limpa, Mesa Limpa e demonstrados alguns exemplos.
    - PSI NOVA. Diretriz: A senha não poderá ser de fácil dedução. Como conter parte do próprio nome ou nomes de familiares e animais de

estimação ou datas comemorativas. Senhas populares deverão ser evitadas para dificultar ataques de dicionário;

- PSI NOVA. Diretriz*: A Royal Magnífica adota a política de Tela Limpa, Mesa Limpa, onde se dever evitar manter anotadas as senhas em papel, postit, arquivos, dispositivos móveis, etc, de fácil acesso a terceiros;*

- PSI ANTIGA - A senha possui validade de 90 dias. Ao término desse período, será automaticamente solicitada a sua troca.
    - COMENTÁRIO: Nessa diretriz foi alterado o prazo de validade da senha de 90 para 60 dias.
    - PSI NOVA. Diretriz: A senha por padrão tem a data de 60 dias de expiração. Ao vencer essa data será automaticamente bloqueado o acesso forçando a criação de uma nova;
- PSI ANTIGA - Para efeito de histórico, são armazenadas as sete últimas senhas utilizadas, não sendo permitido o seu uso para a gravação de uma nova senha.
    - COMENTÁRIO: Foi aumentado o limite de 7 para as 10 últimas senhas utilizadas para acesso à rede. Assim forçando o usuário a utilizar novas senhas por um longo período de tempo.
    - PSI NOVA. Diretriz: *O sistema guardará as 10 últimas senhas, restringindo assim a repetição delas nesse período*

O novo documento de Política de Segurança da Informação está disponibilizado no Apêndice A para a comparação com a sua antiga versão que se encontra no Anexo B.

4 PROCESSO DE CAMPANHA E SEU DESENVOLVIMENTO

Neste capítulo será abordado o desenvolvimento da proposta do estudo de caso da campanha de educação institucional em segurança da informação e da comunicação da Política de Segurança da Informação e o seu desenvolvimento ao longo desse percurso. Dividido em partes que contemplam a escolha do tema da primeira campanha, a comunicação das partes envolvidas, a elaboração da estratégia de divulgação na empresa e a elaboração do cronograma de apresentação da campanha.

Essa primeira parte demonstra a definição do tema da campanha realizada para a educação em segurança da informação e da comunicação da nova PSI aos colaboradores da empresa, que, após a gerência de tecnologia em posse dela concluída e assinada pela alta gestão deverá ser comunicada aos usuários através de uma campanha envolvendo também um treinamento em segurança da informação para que eles tenham ciência dos regulamentos exigidos pela organização e das suas penalidades.

A norma ABNT ISO/IEC 27002:2013 (2013b, p20) define em um de seus controles a utilização de campanhas e treinamentos de segurança da informação aos usuários da empresa, ela orienta:

> Convém que todos os funcionários da organização e, onde pertinente, partes externas devem recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

O Grupo de Construção das Políticas e Normas de Segurança da Informação ao fim da conclusão da etapa de produção da PSI junto com o gerente da GEINF se reuniram para traçar a nova etapa da divulgação deste documento e do treinamento em segurança aos usuários. Sabendo que na corrente de segurança a parte mais fraca é o usuário, deste modo, ele deverá também ser instruído em assuntos de segurança da informação para que no seu proceder diário evite expor a organização a riscos e até mesmo quebre regulamentos de segurança. A revista

digital Computerworld.com.br publicou uma matéria de RODRIGUES (2016) sobre cibercrime informando essa preocupação dos gestores para com os usuários:

> Executivos de TI estão cada vez mais preocupados com seus próprios funcionários, que são como inocentes portas de entrada com altos níveis de privilégio. Em 2016, as empresas devem dar mais importância à educação do usuário final, percebendo que, independentemente do quanto invistam em segurança, os usuários podem colocar tudo a perder se não colocarem as regras em prática.
>
> O envolvimento em processos de segurança, a obediência às políticas de segurança (que deverão ser definidas, caso ainda não existam) e a capacidade de reconhecer e-mails de *phishing* e outras armadilhas serão essenciais no processo. Afinal, é impossível impedir que os usuários errem, mas é possível educá-los, monitorá-los e analisar a maneira como usam os dados para flagrar vulnerabilidades e ataques.

Diante dessa preocupação, a necessidade era começar com assuntos de mais vivencia dos usuários, ou seja, atividades que impactam diariamente com seus serviços, algo que eles estão acostumados a fazer todos os dias. A proposta da campanha ser voltada para a segurança em senhas foi interessante por ela cobrir esses requisitos. A política anterior não tinha regulamentos rígidos no tratamento dessa informação e da sua alta importância. Após estabelecido o tema, o nome definido foi “Sua Senha, Nossa Segurança”, que foi validado pelos integrantes do grupo de construção e definido para o então estudo.

Como regra da empresa Royal Magnífica as gerências que desejarem fazer divulgações de campanhas ou disparar informativos usando qualquer meio da organização (seja ele no mural, e-mail, site, intranet e outros), deverão informar a necessidade para a Gerência de Comunicação Interna - GECOI, que é a definida para essas atividades de comunicação interna da empresa. Seguindo a norma, os gestores das áreas de infraestrutura e de comunicação tiveram três reuniões para acertarem o trabalho entre as equipes para a divulgação da campanha ser iniciado.

No primeiro encontro, a reunião tratou do tema e estabeleceram as formas de comunicação em que seriam divulgadas a campanha de educação em segurança da informação e da divulgação da PSI e o material a ser divulgado nelas. Seguindo a orientação da diretriz constante no controle 7.2.2 da norma ABNT ISO/IEC 27002:2013 (2013b, p.20) que regulamenta sobre a conscientização, educação e treinamento em segurança da informação, indica:

> Convém que o programa de conscientização considere um número de atividades de conscientização, tais como, campanhas (por exemplo, dia da segurança da informação) e a publicação de boletins ou folhetos.

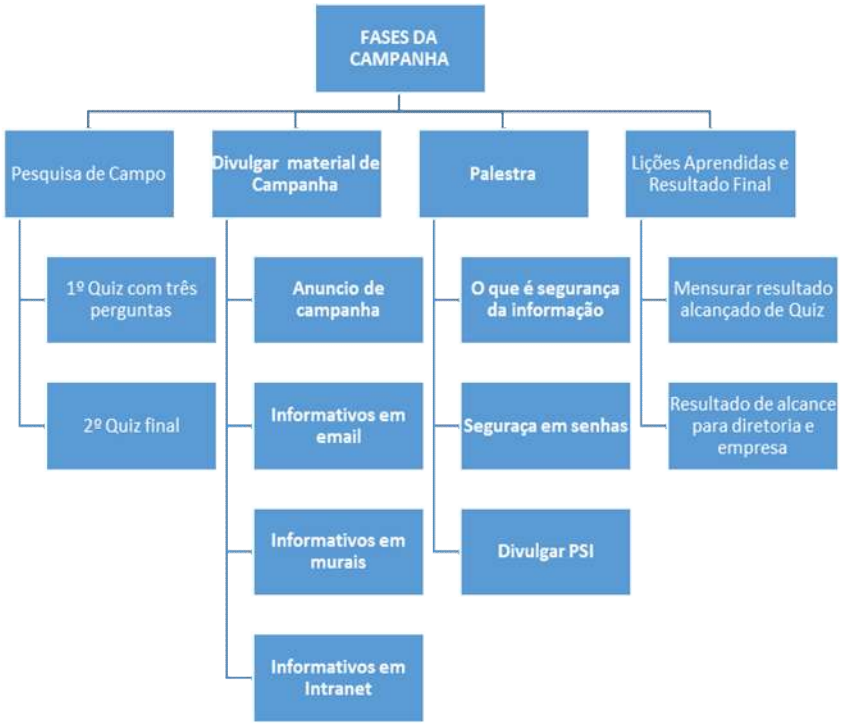
. A forma de comunicação principal foi definida como e-mail, por ser a ferramenta de alcance a todos funcionários da organização e mais a utilização folders em murais na sede da empresa.

Na segunda reunião, a GECOI demonstrou três modelos de cada material elaborado (*folders*, logos, *layouts*, *teasers* e a pesquisa de campo) com as informações para as divulgações montadas pelo Grupo de Construção. O que coube a equipe de construção selecionar a escolha do modelo a ser utilizado em cada material da campanha.

Na terceira reunião, foi apresentado a proposta de divulgação da campanha pela GECOI. Proposta essa validada pelo grupo de construção e pelo gestor da GEINF. Essa Proposta de Campanha se encontra disponível no Anexo A.

Na última parte do desenvolvimento da proposta foi definido o cronograma de apresentação contendo quatro etapas. 1º Pesquisa Institucional, 2º Divulgação de materiais didáticos, 3º Palestra sobre o tema e apresentação da PSI e a 4º Nova pesquisa para mensurar o alcance do tralho e resultado final. O detalhamento de cada parte e a sua estrutura analítica, EAP, se encontra logo abaixo.

FIGURA 4 ESTRUTURA ANALÍTICA DA CAMPANHA



FONTE – ELABORADO PELO AUTOR DO TRABALHO.

- Na primeira etapa foi realizada a pesquisa institucional através de um formulário enviado por correio eletrônico a fim de mensurar a ciência dos usuários sobre os regulamentos da PSI existente;
- A segunda etapa envolveu as divulgações dos materiais de campanha sobre a segurança em senha (os *folders* e *teasers*);
- A terceira etapa se deu com a realização de palestra sobre o tema “Sua Senha, Nossa Segurança” que envolve o tema de educação institucional em segurança da informação e a divulgação da nova PSI aos colaboradores;
- Na quarta etapa, a veiculação de nova pesquisa institucional através de um formulário enviado por correio eletrônico e a divulgação do resultado final das pesquisas.

4.1 A campanha e sua execução

Nesta parte será demonstrado como foi a execução da campanha na empresa Royal Magnífica, os seus números de pesquisas, materiais produzidos, dificuldades, necessidades futuras e a conclusão.

O início da campanha de educação em segurança da informação iniciou com a veiculação por e-mail da primeira pesquisa institucional disponibilizada pela GECOI com o intuito de levantar o percentual de colaboradores que sabiam da existência da Política de Segurança da Informação da empresa e sobre algumas questões de segurança da informação para que ao final da campanha pudesse ser comparado com outra pesquisa de mesma característica e assim mensurar a proficiência do trabalho desempenhado.

A pesquisa foi elaborada de forma simples e direta, com seis questões objetivas (resposta SIM ou NÃO), ficando disponível para o preenchimento do usuário num período de uma semana. Nela foi buscado ter a participação de grande parte do total de colaboradores da empresa, porém, é sabido que muitos colaboradores não são participativos nesses tipos de pesquisas. Portanto, foi considerado como participação satisfatória um mínimo de 20% do total dos 1200 colaboradores da organização. O formulário de pesquisa foi construído na plataforma do Google Formulário, onde este validou os usuários pelo seu login de e-mail corporativo, limitando a somente uma participação por login e em favor do sigilo dos votos não foram registrados quem participava.

O questionário da pesquisa montado apresentava as seguintes questões:

1. A qual setor da empresa você pertence? (Subitens com os nomes dos setores da empresa para a escolha);
2. Você sabia que a empresa Royal Magnífica possuí uma Política de Segurança da Informação?
    a. Sim.
    b. Não.

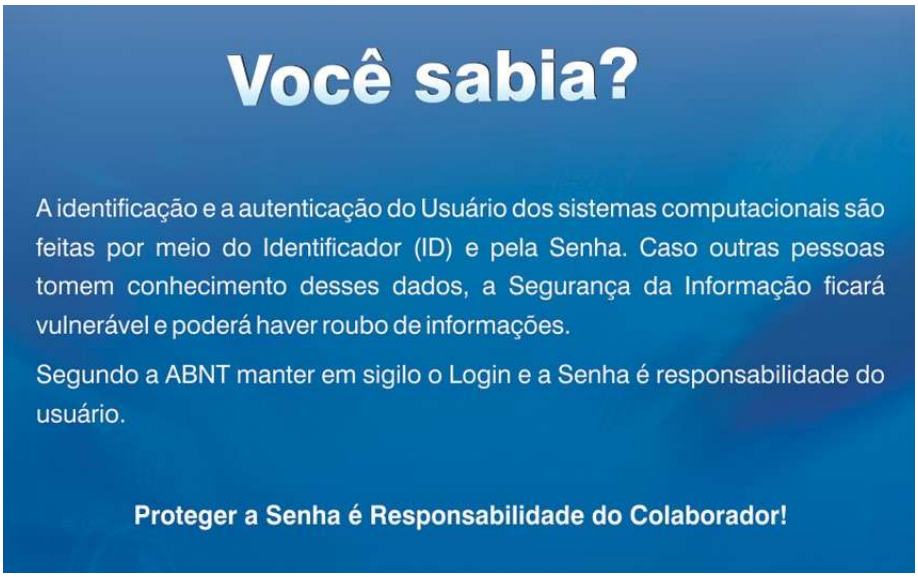
3. Você conhece a Política de Segurança da Informação da Royal Magnífica?
    a. Sim.
    b. Não.
4. Você sabia que todos nós, colaboradores, somos responsáveis por manter o ambiente da rede seguro?
    a. Sim.
    b. Não.
5. Você sabia que as senhas de acesso a sistemas são pessoais e intransferíveis?
    a. Sim.
    b. Não.
6. Uma senha segura é uma senha formada com:
    a. Nomes de familiares, datas comemorativas, nome de animal de estimação?
    b. Frases que contenham letras, números e símbolos?

Após o vencimento do período de uma semana foi retirada do ar a pesquisa e iniciado a análise dos seus dados. No total de participações, foi obtido o resultado satisfatório de 25% dos colaboradores participantes. Com cerca de 80% dos colaboradores dizem saber da existência da política de segurança. Cerca de 65% dizem conhecer a política de segurança. Ainda 95% deles afirmam saber que são responsáveis pela segurança da informação e 98% também dizem saber que as senhas de acesso a sistemas são pessoais e intransferíveis. E por último, 63% dos participantes disseram que frases que contenham letras, números e símbolos são mais seguros que formada com nomes de familiares, de animal de estimação e datas comemorativas.

Na próxima etapa, foi iniciado o processo da divulgação dos materiais de educação em segurança da informação com o assunto em segurança em senhas,

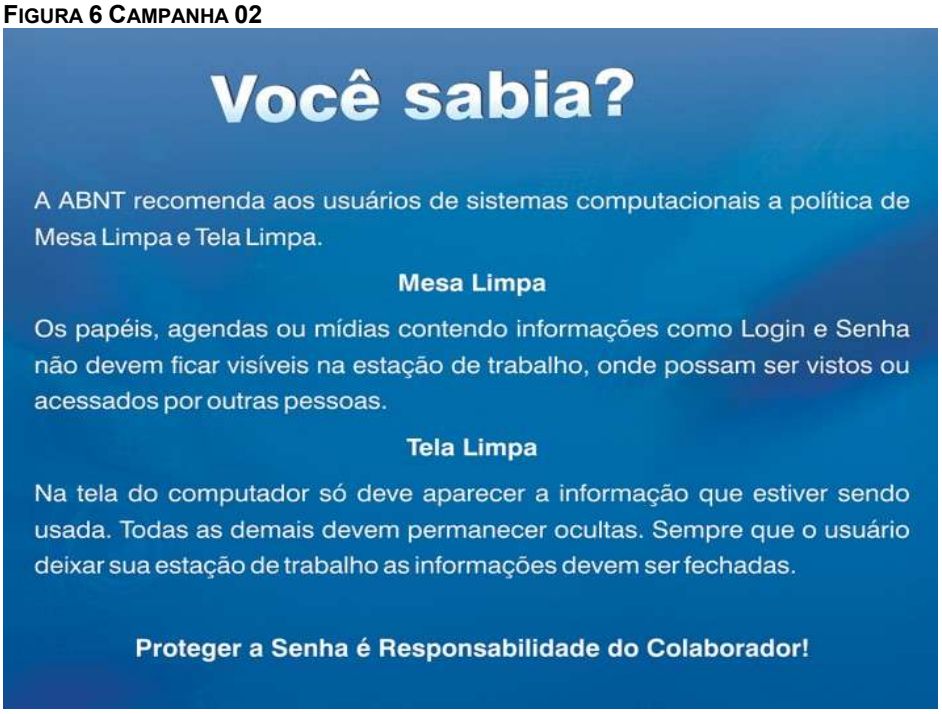
sobre o tema Sua Senha, Nossa Segurança. Os materiais utilizados como base de instrução foram os fascículos da Cert.br e da norma ABNT NBR ISO/IEC 27002:2013. Nesta etapa foram enviados em datas programadas os *folders* e *teasers* produzidos pela GECOI aos e-mails dos colaboradores e disponibilizados também em intranet e no mural das áreas de convivência e copas da empresa. Os cartazes foram afixados nos murais de acordo com os temas que iam sendo lançados. De maneira a concentrar a informação nos locais onde os usuários que dispunham uma parte do seu tempo dentro da organização pudessem ler a informação ali também. O cronograma das datas poderá ser conferido na Proposta de Campanha, no Anexo A, e algumas das imagens dos *folders* produzidos (devidamente recortado a logo da campanha e da empresa) estão dispostos logo abaixo.

FIGURA 5 CAMPANHA 01



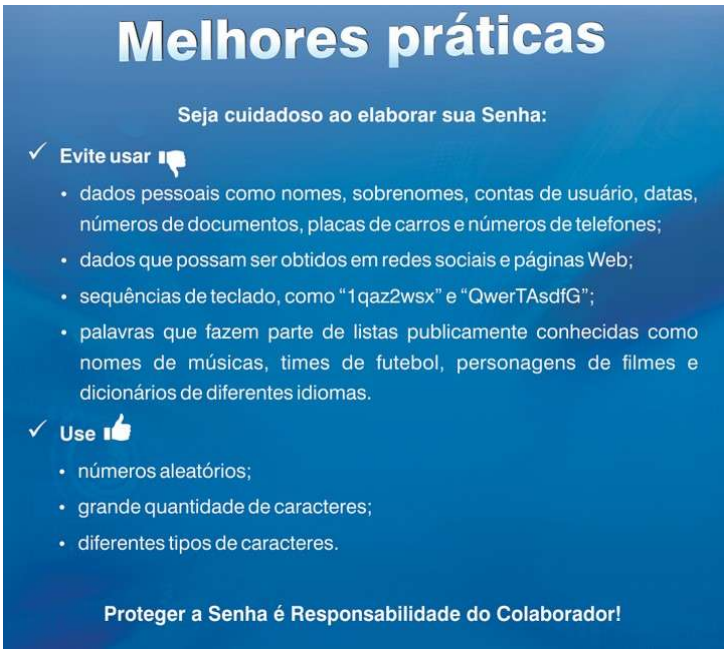
FONTE – ELABORADO PELO AUTOR DO TRABALHO.

FIGURA 6 CAMPANHA 02



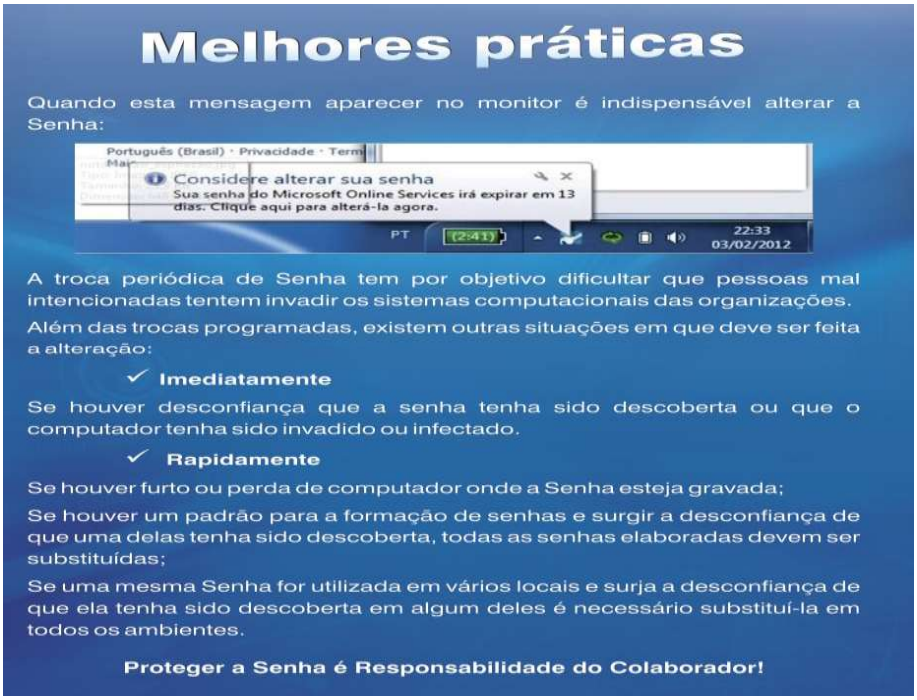
FONTE – ELABORADO PELO AUTOR DO TRABALHO.

FIGURA 7 CAMPANHA 03



FONTE – ELABORADO PELO AUTOR DO TRABALHO.

FIGURA 8 CAMPANHA 04



FONTE – ELABORADO PELO AUTOR DO TRABALHO.

As mensagens construídas nos *folders* e *teasers* trouxeram informações sobre: a importância de uma senha forte para um ambiente tecnológico empresarial, como se criar uma senha, erros mais comuns ao se criar uma senha, de quem é a responsabilidade da gestão de senha e a necessidade de ser atualizada periodicamente. Assim igualmente nos cartazes disponibilizados. Esta etapa teve um período de duração de 25 dias.

Ao fim do processo da divulgação dos materiais de educação foi iniciado a terceira etapa em que foram realizadas as atividades de palestras aos colaboradores. Nessa etapa tiveram três turmas por dia ao longo de uma semana. As palestras ocorreram no auditório próprio da organização com cerca de 60 pessoas participantes por turma e com duração de cerca de 50 minutos cada, assim contemplando a participação de todos os colaboradores da sede, em Brasília.

Essa etapa realizada teve o apoio e participação do gestor da GEINF - onde ministrou sobre o tema da campanha e apresentou a nova Política de Segurança da Informação, do diretor de tecnologia - onde ele endossou a importância de todo o corpo de funcionários a seguirem a Política de Segurança e adotarem as melhores práticas em segurança da informação para a saúde e segurança da empresa, além do apoio e suporte da equipe de construção da PSI que fizeram parte nas respostas de dúvidas, informações e sugestões.

A apresentação da palestra foi dividia em três momentos. No primeiro instante o gestor da GEINF abordou os temas: O que é segurança da informação, O valor da informação para a organização, A nova Política de Segurança da Informação, Tópicos interessantes a serem comentados sobre a nova PSI - O que mudou? Nesse tópico também abordado sobre o controle de senhas e métodos de segurança que deverão ser adotados pelos colaboradores.

No segundo momento a palavra com o Diretor de Tecnologia - DITEC, que discorreu brevemente sobre a importância da participação dos usuários da organização e salientou que a alta gestão estava compromissada com o tema de segurança da informação e, por fim, agradece a presença e colaboração de todos eles.

No terceiro e último momento, foi disponibilizado no final da palestra dez minutos para que os usuários pudessem interagir com toda a equipe organizadora (gerente, grupo de construção e diretor) a fim de tirarem as suas dúvidas, informações e sugestões da PSI. Algumas das palestras não tiveram participações registradas, porém das que ocorreram algumas dessas perguntas foram semelhantes como “Não vou poder carregar o meu celular mais pela porta USB do computador? ”, “Sou obrigado mesmo a mudar constantemente de senha?”, “Já fomos alvos de ataques de *hackers*?”.

A estrutura da palestra seguiu este o modelo descrito a seguir:

1. Apresentação de treinamento em Segurança da Informação aos colaboradores da empresa – sede Brasília.

    a. Palestra de campanha Minha Senha, Nossa Segurança.

1. O que é Segurança da informação;
2. Qual o valor da informação para a organização.
3. Casos de fracassos;
4. A nova Política de Segurança da Informação.
5. Tópicos interessantes da PSI – O que mudou?
    1. Exemplos da Norma e de procedimentos adotados pela Empresa.
    2. Bloqueio de USB.
    3. E-mail;
    4. Senha de rede.

b. Importância da participação dos colaboradores da organização;
    1. Torna o ambiente seguro.
    2. Traz novos clientes. (Imagem da empresa).

c. Perguntas, dúvidas e respostas.

QUADRO 1 REGISTRO DE PARTICIPAÇÕES DAS PALESTRAS

PERIODO DE TURMA	SEGUNDA - FEIRA	TERÇA - FEIRA	QUARTA – FEIRA	QUINTA – FEIRA	SEXTA - FEIRA
1º TURMA	Não vou poder carregar o meu celular mais pela porta USB do computador?	Vou ter que mudar a senha periodicamente mesmo?		Por que celular pessoal não pode ser configurado o e-mail da empresa?	Sou obrigado mesmo a mudar constantemente de senha?
2º TURMA	Sou obrigado mesmo a mudar constantemente de senha?	Todos somos obrigados a seguir essas regras?			Já fomos alvos de ataques de hackers?

3º TURMA	Sou obrigado mesmo a mudar constantemente de senha?	Sou obrigado mesmo a mudar constantemente de senha? Já fomos alvos de ataques de hackers?	Não vou poder carregar o meu celular mais pela porta USB do computador? Por que celular pessoal não pode ser configurado o e-mail da empresa?		

Fonte – elaborado pelo autor do trabalho.

Por fim, na quarta etapa, foi encaminha uma nota por e-mail agradecendo a todos colaboradores por terem participado da campanha lendo os e-mails e indo a palestra realizada. Por oportuno, também acompanhado a este e-mail a última pesquisa institucional para obtenção dos resultados alcançados com a campanha. A pesquisa ocorreu de igual modo a primeira veiculação, porém, algumas das questões foram específicas para a pós campanha. O questionário da pesquisa montado apresentava as seguintes questões:

1. A qual setor da empresa você pertence? (Subitens com os nomes dos setores da empresa para a escolha);
2. Você sabia que a Política de Segurança da Informação era importante para uma organização?
    a. Sim.
    b. Não.
3. Você conhece os controles estabelecidos na nova Política de Segurança da Informação da Royal Magnífica?
    a. Sim.
    b. Não.
4. Uma senha segura é uma senha formada com:

   a. Nomes de familiares, datas comemorativas, nome de animal de estimação?

   b. Frases que contenham letras, números e símbolos?

5. Qual a avaliação que você daria para a campanha de educação em segurança da informação da Royal Magnífica?

   a. Boa.

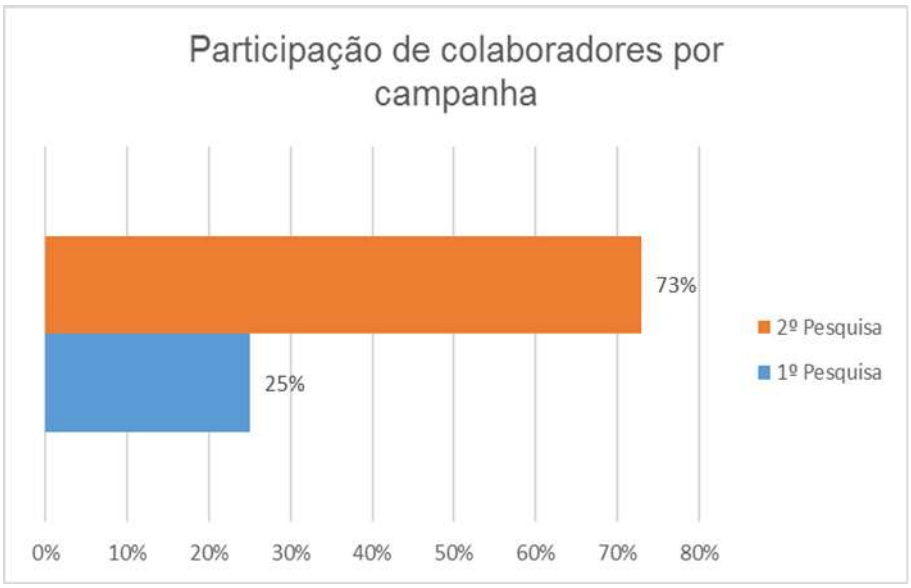
   b. Média.

   c. Ruim.

6. Sugestões para uma próxima campanha.

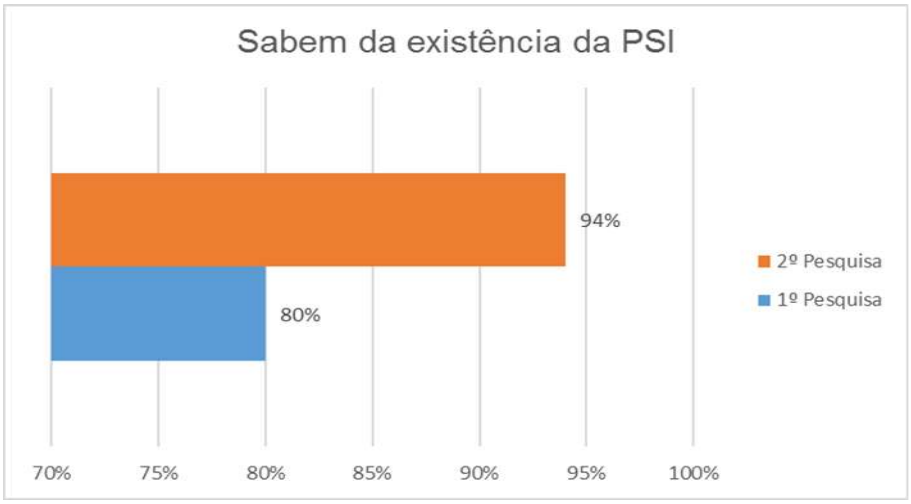
Esta pesquisa também ficou disponível no período de uma semana e os seus resultados foram satisfatórios. A pesquisa alcançou 73% de participação pelos colaboradores. Dentre esses, 94% afirmaram saber que a Política de Segurança da Informação é importante para a organização, 87% afirmaram que conheciam os controles estabelecidos por ela, e 98% dos participantes afirmaram que a senha segura é aquela formada por frases que contenham letras, números e símbolos. E na avaliação tivemos o resultado de 74% nota Boa, 26% de nota Média e 0% de nota ruim. Logo a baixo está apresentado os gráficos dos resultados obtidos pelas campanhas.

FIGURA 9 TOTAL DE PARTICIPAÇÃO DE COLABORADORES POR CAMPANHA



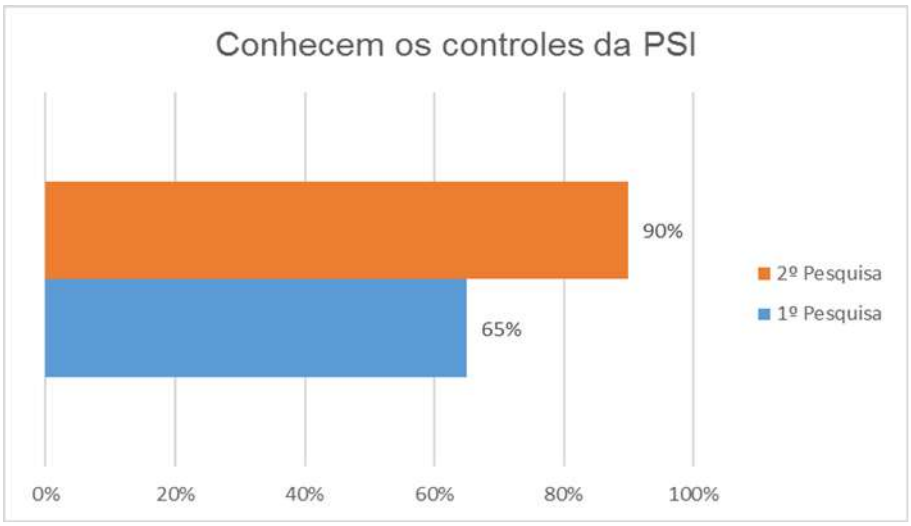
FONTE – ELABORADO PELO AUTOR DO TRABALHO.

FIGURA 10 COLABORADORES QUE SABEM DA EXISTÊNCIA DA PSI



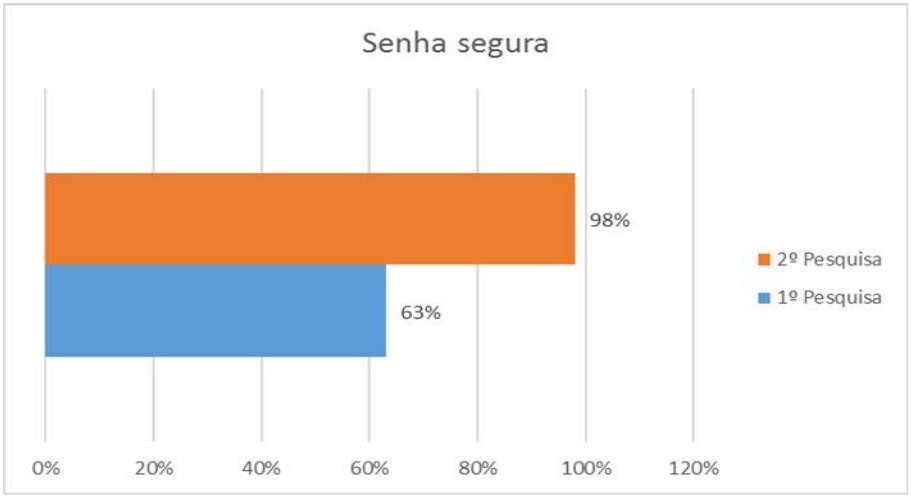
FONTE – ELABORADO PELO AUTOR DO TRABALHO.

FIGURA 11 TOTAL DE COLABORADORES QUE CONHECEM OS CONTROLES DA PSI



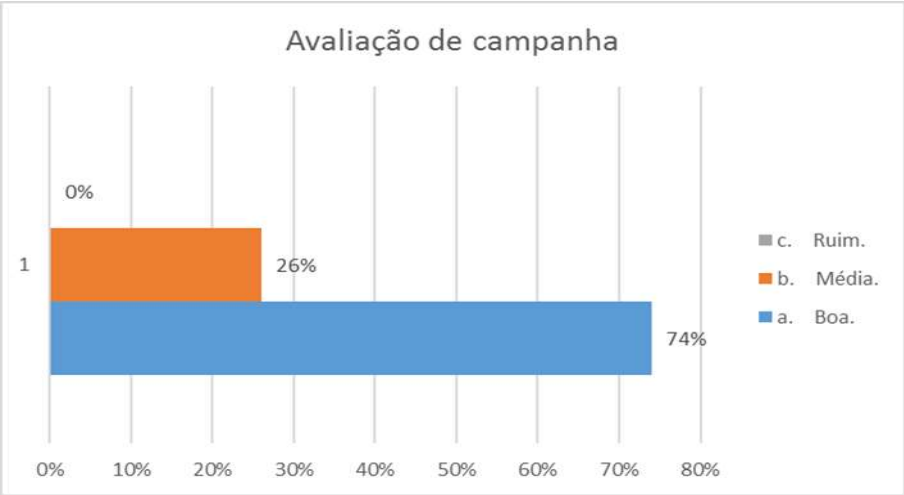
FONTE – ELABORADO PELO AUTOR DO TRABALHO.

FIGURA 12 SENHA SEGURA



FONTE – ELABORADO PELO AUTOR DO TRABALHO.

FIGURA 13 AVALIAÇÃO DE CAMPANHA



FONTE – ELABORADO PELO AUTOR DO TRABALHO.

O resultado mensurado da campanha teve o sucesso esperado em número de participações de colaboradores. Na primeira pesquisa realizada se teve um total de 25% (que já era bom) e na segunda 73% de participantes do total de 1200 colaboradores, uma diferença de 48% de participações. Teve um crescimento de 14% de colaboradores que disseram conhecer a Política de Segurança da organização e um aumento de 25% de colaboradores que agora de fato conhecem os regulamentos existentes na Política de Segurança. E na pergunta de que forma uma senha segura é formada teve-se 35% de respostas a mais do que na primeira vez que foi questionado.

Em posse do resultado dos dados das pesquisas foi editado o documento do relatório final e entregue a diretoria de tecnologia para a sua validação e publicação nos meios próprios da empresa, a intranet e e-mail.

A GEINF e a DITEC não têm o intuito de abandonar a campanha de educação e conscientização em segurança da informação aos usuários ao término desse estudo de caso. Visto que os resultados foram positivos e a conscientização e educação tem de ser tarefas contínuas na empresa por motivos de que há sempre um fluxo de novos usuários e novas tecnologias e as necessidades em si se renovam constantemente. E, sim, estabelecer no cronograma institucional a semana

da segurança da informação e nela desenvolver um trabalho como este buscando sempre inovar e aprimorar seus trabalhos com as lições aprendidas.

CONCLUSÃO

De acordo com o que foi demonstrado nesse estudo de caso, concluímos que, uma empresa não poderá de forma alguma, se ausentar da obrigação de implementar processos para o gerenciamento da segurança das suas informações, isso envolve desde a criação de um SGSI, documento de regulamentos (Política de Segurança da Informação), comunicação aos usuários, gerenciar os riscos, fazer a análise de riscos. Como dito por FONTES (2012) a informação é pilar para o sucesso e continuidade de uma organização, por isso, a organização tem de ter uma Política de Segurança eficiente e eficaz para fornecer a proteção desejada a essa informação. Diante disso, todo investimento com processos e regulamentos, equipamentos de segurança e campanhas de conscientização são grandes investimentos se comparado com a perca de capitais e de bens intangíveis que a organização poderá ter num evento de segurança, caso não tenha se precavido com medidas de segurança anteriormente.

O processo de construção de uma PSI não é algo fácil e rápido. Não pode ser simplesmente copiado uma PSI de outra organização e aplicá-la à sua, cada empresa tem a sua particularidade e seus objetivos de negócios podem ser totalmente diferentes uma da outra. A construção de regulamentos é um processo meticuloso e deverá ser analisado caso a caso, feito reuniões com gestores de diversos setores, como o de recursos humanos, jurídico, tecnologia e a alta gestão para o mapeamento das informações necessárias a serem protegidas e de que maneira serão. Deverá ser feita também uma análise de riscos para se levantar com exatidão os riscos existentes na organização para então elaborar sua ação de proteção ou aceitação.

A existência de uma gerência destinada ao tratamento especificamente sobre segurança da informação é imprescindível para que os processos e projetos de segurança da informação sejam elaborados, implementados e atualizados habilmente. Tal qual a importância da existência de um Plano de Continuidade do Negócio – PCN e a existência da gestão de riscos. Os códigos dos sistemas

existentes na organização deverão estar alinhados com as políticas de segurança da organização.

Os regulamentos deverão ser escritos de forma simples, evitando termos muitos técnicos que dificultam a compreensão do usuário. A organização tem de falar conforme a linguagem de entendimento dos usuários. A política é escrita para o usuário e ele deverá a ter como o seu manual de segurança. Um manual de difícil assimilação poderá frustrar toda a intenção, tempo e dinheiro gasto com o seu projeto.

Não o bastante, podemos dizer que os fatores críticos para o sucesso da implantação dos regulamentos é o comprometimento e apoio visível da alta administração, regulamentos devem ter o tratamento verdadeiro que a organização deseja para suas informações e regulamentos que realmente serão efetivos, ou seja, um livro com regras que não são exigidas será um livro que o usuário não levará a sério.

A campanha de conscientização, comunicação e treinamento é fundamental para a expansão do conhecimento das novas normas ou das atualizadas e ajuda no processo de educação e treinamento dos usuários em segurança da informação. Muitos deles não são proficientes em tecnologia da informação, possuem bastante dúvidas nos processos de manutenção da segurança (o que fazer ou como fazer – o que posso e o que não posso) e precisam ser treinados em segurança da informação. Os resultados das pesquisas de campo deste trabalho comprovam a necessidade de campanhas em segurança da informação, antes da campanha 65% dos colaboradores conheciam a Política de Segurança da Informação, ao passo que depois da realização da campanha esse número se elevou para 90%. O mesmo resultado positivo tivemos quando mensurado o número de colaboradores que diziam saber se quer da existência da Política de Segurança da informação, onde tivemos uma porcentagem de 14% a mais do que antes da campanha. Sem contar o número 48% a mais de colaboradores que participaram dos questionários nesse segundo momento.

Por fim, para alcançar o sucesso, a Política de Segurança da Informação deverá progredir associado a uma campanha de segurança e ser comunicada a

todos colaboradores da organização periodicamente no objetivo de manter seus colaboradores treinados e atualizados.

REFERÊNCIAS

ABNT, NBR ISO/IEC 27001:2013 - **Técnicas de Segurança – Sistemas de gestão de segurança da informação** - Requisitos. 2013a

ABNT, NBR ISO/IEC 27002:2005 - **Técnicas de Segurança – Código de Prática para controles de segurança da informação**. 2005.

ABNT, NBR ISO/IEC 27002:2013 - **Técnicas de Segurança – Código de Prática para controles de segurança da informação**. 2013b.

BASTOS, Alberto; CAUBIT, Rosângela. **ISO 27001 e 27002**: gestão de segurança da informação - uma visão prática. Porto Alegre, Zouk, 2009.

CARBONE; Fernando, **10Minutos sobre Segurança da Informação**, 2014. PWC . Disponível em: <http://www.PWC .com.br/pt/10minutes/2014/PWC -10minutos-seguranca-informacao-14.html> Acesso em: 14 abr. 2016.

FERNANDES, Aguinaldo Aragon. **Implantando a governança de TI**: da estratégia à gestão dos processos e serviços, 3.ed. Rio de Janeiro: Brasport, 2012.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Marcio Tadeu. **Política de Segurança da Informação**: Guia Prático para Embalagem e Implementação. Rio de Janeiro, Ciência Moderna, 2006

FONTES, Edison. **Segurança da Informação: o usuário faz a diferença!** Disponível em: http://www.viaseg.com.br/artigos/artigo_edison_051125.htm Acesso em: 02 maio 2016.

FONTES, Edison. **Políticas e Normas para a Segurança da Informação**. Brasport, 2012.

ISO/IEC 27000:2016(en) **- Information technology — Security techniques — Information security management systems — Overview and vocabular.** 2016.

MARTINS, José Carlos Cordeiro. **Gestão de Projetos de Segurança da Informação**. Rio de Janeiro, Brasport, 2013.

MITNICK, Kevin. **A arte de enganar**. São Paulo: Pearson Education do Brasil Ltda, 2003.

MODULO. **Conscientização de usuários: como envolver seu público com a Segurança da Informação**. Disponível em: <http://www.modulo.com.br/comunidade/entrevistas/616-conscientizacao-de-usuarios-como-envolver-seu-publico-com-a-seguranca-da-informacao> Acesso em: 02 maio 2016.

OLIVEIRA, Viviane. **10Minutos sobre Segurança da Informação**, 2014. PWC .

Disponível em: <http://www.PWC .com.br/pt/10minutes/2014/PWC -10minutos-seguranca-informacao-14.html> Acesso em: 14 abr 2016.

RODRIGUES, Carlos. **Segurança: Veja quatro previsões sobre ramsonware e violações**. Disponível em: http://computerworld.com.br/seguranca-veja-quatro-previsoes-sobre-ramsonware-e-violacoes Acesso em: 02 abr 2016.

SÊMOLA, M. **Gestão da Segurança da Informação: Uma visão executiva.** Rio de Janeiro, Editora Campus, 2003;

PWC (2016). **10minutos sobre Pesquisa Global de Segurança da Informação 2016**. PricewaterhouseCoopers, 2016. Disponível em: http://www.PWC .com.br/pt/10minutes/assets/2016/PWC -10min-pesq-global-seg-inf-16.pdf. Acesso em: 20 mar 2016.

APÊNDICE A – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Política de Segurança da Informação

ROYAL MAGNÍFICA

[Versão 1]

OBJETIVO

Este documento define o tratamento que deve ser dado às informações armazenadas ou transmitidas no ambiente convencional ou tecnológico da ROYAL MAGNÍFICA.

Todas as orientações aqui apresentadas são os princípios fundamentais e as diretrizes básicas que possibilitam que a informação tenha garantida a sua confidencialidade, integridade e disponibilidade.

As orientações descritas nessa norma representam como a organização exige que a informação seja utiliza e tratada.

Para a ROYAL MAGNÍFICA todo ativo de informação é um o conjunto de informações, armazenadas de modo que possa ser identificada e reconhecida como valiosa para a empresa. E Informação é o resultado de processamento e organização de dados (eletrônicos ou físicos) ou registros de um sistema, composto por dados, mas um conjunto de dados não necessariamente é considerado uma informação.

APLICABILIDADE

Essa Política se aplica a todos os colaboradores, estagiários, menores aprendizes e prestadores de serviço que exercem atividades no âmbito da ROYAL MAGNÍFICA. Ou qualquer um que venha a ter acesso a dados ou informações da empresa.

TERMINOLOGIAS

Ativo: Qualquer coisa que tenha valor para a organização [ISO/IEC 13335- 1:2004].

Disponibilidade: Propriedade de que a informação esteja acessível e utilizável quando requerida por uma pessoa física ou sistema, órgão ou entidade.

Integridade: Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

Confidencialidade: Propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização para pessoas, entidades ou processos.

Software: Programa de computador.

Hardware: Parte física do computador, ou seja, é o conjunto de componentes eletrônicos, circuitos integrados e placas.

Usuários: Pessoas que utilizam os recursos tecnológicos de propriedade ou controlados pela organização. Exemplo: colaboradores, estagiários, menores aprendizes e prestadores de serviço.

ATRIBUIÇÕES

A alta direção é responsável por aprovar e prover recursos necessários para aplicabilidade da Política de Segurança da Informação.

Os profissionais de tecnologia da Informação são responsáveis pela implementação, implantação e compreensão da Política de Segurança da Informação.

Os profissionais da área jurídica são responsáveis por analisar a conformidade da Política de Segurança com a legislação vigente.

Os custodiante ou detentores de informação são responsáveis pela classificação, reclassificação e guarda das informações que lhes pertencem.

Os usuários são responsáveis por utilizar os sistemas de informação e os recursos computacionais somente para os fins previstos pela Política de Segurança.

DIRETRIZES

A informação é um patrimônio que deve ser protegido de acordo com a sua classificação;

A informação constante nos seus formatos físico ou lógico e os periféricos tecnológicos utilizados pelos usuários são de exclusiva propriedade da ROYAL MAGNÍFICA, não podendo ser interpretados como de uso pessoal;

As informações, os recursos e sistemas de informação e os recursos da ROYAL MAGNÍFICA e sob sua guarda devem ser protegidos contra ameaças (naturais, acidentais ou intencionais), de forma a reduzir os riscos e garantir a confidencialidade, integridade e disponibilidade (CID);

Deverão ser estabelecidos controles apropriados de auditoria em todos os sistemas em que a instituição achar necessário, para minimizar os riscos dos seus ativos de informação;

A segurança da informação é uma responsabilidade de todos que integram a ROYAL MAGNÍFICA e cada um deve estar atento em preservá-la.

O acesso à rede e aos sistemas da empresa ROYAL MAGNÍFICA será feito por meio de login de acesso único, pessoal e intransferível;

As senhas de acesso a sistemas deverão ser formadas rigorosamente por frases que contenham caracteres alfanuméricos e símbolos;

Os acessos aos funcionários e prestadores de serviços devem ser solicitados e aprovados somente às informações necessárias ao desempenho de suas atividades;

A ROYAL MAGNÍFICA poderá utilizar de quaisquer recursos para monitorar e controlar o conteúdo e o acesso à informação da sua infraestrutura;

O usuário é totalmente responsável pela segurança de cada informação da ROYAL MAGNÍFICA, especialmente daquelas que estão sob sua responsabilidade;

O usuário é responsável pela conta de correio eletrônico que lhe foi disponibilizada pela ROYAL MAGNÍFICA. As mensagens do correio eletrônico deverão ser escritas em linguagem profissional e de forma que não comprometa a imagem da organização. E todo o seu conteúdo poderá ser acessado e monitorado pela organização quando em situações que ponham em risco a sua imagem, negócio e sua lucratividade;

O ambiente de Internet deve ser usado para o desempenho das atividades profissionais do usuário para a ROYAL MAGNÍFICA. E todos os acessos realizados nesse ambiente são monitorados pela organização;

Deverão ser implantados, revisados e testados periodicamente planos de contingência e de continuidade para os sistemas da ROYAL MAGNÍFICA;

Deverão ser implantados sistemas de segurança lógica e física para a proteção dos ativos da informação e ferramentas de prevenção e monitoração de intrusão nos ambientes digitais;

O recebimento e a instalação de produtos de hardware ou software nos ambientes da ROYAL MAGNÍFICA devem ser formalizados por contrato, inclusive nas situações caracterizados como testes;

Os usuários devem seguir as orientações de segurança da ROYAL MAGNÍFICA e adotar os controles de segurança definidos e disponíveis para a proteção dos recursos sob sua responsabilidade;

No processo de gestão, custódia e uso das informações a ROYAL MAGNÍFICA garante à preservação da sua confiabilidade, considerando proibido tudo aquilo que não for explicitamente permitido;

Somente as pessoas autorizadas, formalmente autorizadas, deverão ter acesso às informações e aos ambientes tecnológicos da ROYAL MAGNÍFICA;

Deverão ser tomadas atitudes para evitar ataques de engenharia social;

A sala de tecnologia da ROYAL MAGNÍFICA tem ambiente controlado no padrão 24/7 por meio de câmeras de monitoramento, aparelho de medição de umidade do ar e acesso limitado por chave e fechadura de liberação por senha de conhecimento apenas do pessoal autorizado;

Todos os funcionários e prestadores de serviço da ROYAL MAGNÍFICA devem assinar Termo de Compromisso quanto ao sigilo dos dados, informações e conhecimentos da ROYAL MAGNÍFICA, o Termo de Recebimento de Estação de Trabalho e/ou Termo de Recebimento de Aparelho Telefônico ou Tablet;

Todos os usuários devem ser conscientizados e treinados nos procedimentos de segurança da informação;

O uso indevido ou não autorizado dos ativos e dos recursos de tecnologia da informação e a ação em desacordo desta norma pelo usuário ficarão sujeitos à aplicação das penalidades previstas em legislação pertinente;

Essa Política de Segurança da Informação deve ser revisada e atualizada periodicamente a cada ano, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

CONCLUSÃO

Todos os usuários devem utilizar a informação de acordo com as determinações desta Política de Segurança.

A segurança e proteção da informação é uma responsabilidade continua de cada usuário da ROYAL MAGNÍFICA.

A Gerência de Tecnologia – GETEC é a área responsável pela existência e ética do processo de proteção e segurança da informação da ROYAL MAGNÍFICA.

O não cumprimento dessa Política e/ou dos demais instrumentos normativos que complementarão o processo de segurança constitui falta grave, e o usuário está sujeito a penalidades previstas na legislação pertinente.

REFERENCIAS

A Política de Segurança da Informação da ROYAL MAGNÍFICA tem como base a Norma Brasileira ABNT NBR ISO/IEC 27002:2013 - Esta norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a Gestão de Segurança da Informação em uma Organização.

VIGÊNCIA

Esta Política de Segurança da Informação entra em vigor na data de sua publicação.

Versão: 01

_____

Assinatura do Diretor responsável

Brasília, de de 2016.

APÊNDICE B – NORMAS E DIRETRIZES

Normas e diretrizes da Empresa Royal Magnífica

ACESSO A INFORMAÇÃO

Objetivos:

Definir o como deverá ser tratada a informação pela organização.

Diretrizes:

- A informação é um ativo que tem valor para a empresa Royal Magnífica. Ela deve ser protegida de maneira que seja garantida a sua disponibilidade, integridade, confidencialidade e autenticidade;
- Toda informação da organização deverá ter um gestor indicado formalmente pela diretoria responsável;
- Os acessos às informações e seu nível de permissão serão concedidos somente por meio de solicitação formal do gestor da informação;
- Cabe ao gestor da informação classificar o nível de confidencialidade e proteção da informação;
- Toda informação crítica para o funcionamento da Royal Magnífica deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto e com proteção adequada;
- O gestor da informação é responsável pela validação periódica dos usuários que possuem acesso à informação sob sua responsabilidade;
- Quando da mudança de setor dentro da Royal Magnífica, o gestor da informação deverá solicitar a exclusão de acesso às informações que são de sua responsabilidade;

- A Royal Magnífica segue a premissa que “Tudo é proibido a menos que expressamente permitido”;
- Os usuários ficam restringidos a acessarem somente as informações necessárias para desempenharem suas tarefas e de utilizar somente dispositivos (equipamento de TI, equipamento de telefonia, aplicações, etc) que necessita para desempenhar sua tarefa/função ou papel na Royal Magnífica;
- A GEINF é a área responsável pela execução da liberação do acesso à informação.

ACESSO A REDE E AOS SERVIÇOS DE REDE

Objetivos:

Definir o acesso as informações e aos recursos de processamento das informações.

Diretrizes:

- Os acessos à rede da Royal Magnífica somente serão concedidos através da solicitação formal do gestor do usuário feita pelo sistema de chamado;
- O acesso à rede da Royal Magnífica somente poderá ser concedido para fins de trabalho profissional de interesse da empresa;
- É proibido conectar computador ou qual quer outro dispositivo particular em cabeamento estruturado e/ou wireless da empresa. As exceções deverão ser analisadas pela GEINF;
- Os dispositivos móveis da empresa têm acesso à rede wireless liberado para fins profissionais;
- A rede wireless disponibilizada para clientes são de uso restrito a eles, não podendo ser conectado dispositivo particular ou empresarial;

- A rede wireless validará a conexão mediante senha e registro de Mac de dispositivo cadastrado em sistema de gerenciamento;
- Toda conexão wireless disponibilizada para terceiros ou prestadores de serviço deverá ter data de expiração para bloqueio e remoção de acesso da rede;
- A rede wireless deverá ser dividida em ambiente corporativo e público;
- Os acessos externos a sistema internos da Royal Magnífica serão permitidos somente por ferramentas homologadas pela GEINF e mediante login e senha de rede da empresa;
- A autenticação do usuário na rede se dará por meio de login único e senha pessoal e intransferível;
- Será removido e bloqueado todo acesso de funcionário à rede que não fizer mais parte organização e de terceiros após o encerramento de suas atividades, contratos ou acordos;
- A rede interna será protegida por ferramenta de filtragem e analise de pacotes;
- Será garantido que todo login de usuário seja único;
- O usuário deverá bloquear a estação de trabalho e/ou seus dispositivos móveis sempre quando se ausentar deles;
- A GEINF se guarda do direito de monitorar todos os acessos e tráfegos de dados na rede da empresa;

DIREITOS EM ACESSOS PRIVILEGIADOS

Objetivos:

Definir que os acessos a privilegiados a sistemas da organização.

Diretrizes:

- As permissões de acessos na Royal Magnífica se dão em dois tipos: administrador (usuários com privilégios de administração do sistema operacional, sistema de gerenciamento de banco de dados ou de aplicação), usuário (privilégio de leitura e execução de informações e sistemas);
- Os direitos de acesso com privilégio de administrador serão concedidos aos usuários conforme a necessidade de uso e com base em eventos alinhados com a política de acesso a informação;
- Todos os usuários da Royal Magnífica são, por padrão, cadastrados com privilégio de usuário;

SEGURANÇA EM SENHAS

Objetivos:

Definir os requisitos da elaboração das senhas, o tratamento de segurança pela organização e as responsabilidades dos seus proprietários.

Diretrizes:

- A guarda, sigilo e proteção da senha é de responsabilidade total do seu proprietário. Ela é pessoal e intransferível, a quebra da sua confidencialidade poderá incorrer em medidas administrativas;
- A senha de acesso a rede das Empresas Royal Magnífica deverá possuir o tamanho mínimo de 7 caracteres e ser utilizado caracteres alfanuméricos e símbolos;
- É obrigatória a troca da senha no primeiro logon na rede, exceto casos de usuários em locais sem domínio de rede;
- A senha não poderá ser de fácil dedução. Como conter parte do próprio nome ou nomes de familiares e animais de estimação ou datas comemorativas. Senhas populares deverão ser evitadas para dificultar ataques de dicionário;

- Deverá ser alterada a senha sempre que houver suspeita de quebra de confidencialidade;
- A senha por padrão tem a data de 60 dias de expiração. Ao vencimento será automaticamente bloqueado o acesso forçando a criação de uma nova;
- O sistema guardará as 10 ultimas senhas, restringindo assim a repetição delas nesse período;
- O usuário tem a cinco tentativas de autenticação na rede sem êxito. Após isso, será bloqueada a conta referente;
- As estações de trabalho permanecerão por 5 minutos em estado de inatividade, após isso a seção do usuário será bloqueada;
- Os usuários que tiverem as senhas bloqueadas por excederem as tentativas de autenticação deverão solicitar o desbloqueio e/ou o reset da senha para GEINF por telefone ou por chamado de outro usuário em sistema padrão;
- Os usuários que tiverem em período de férias, licenças ou afastamento da empresa terão seus logins bloqueados. Devendo o seu gestor solicitar o desbloqueio de rede pelo sistema de chamado quando este usuário estiver de volta ao trabalho;
- A Royal Magnífica adota a política de Tela Limpa, Mesa Limpa, onde se dever evitar manter anotadas as senhas em papel, postit, arquivos, dispositivos móveis, etc, de fácil acesso a terceiros;
- Em situação que funcionário ou terceiro que esteja saindo da empresa tenha conhecimento de senhas de sistemas ou usuários estas deverão ser alteradas após o encerramento das suas atividades.

ACESSO REMOTO

Objetivos:

Definir as condições e restrições para acesso remoto aos sistemas da organização.

Diretrizes:

- Os usuários não podem se conectar a computadores da rede Royal Magnífica ou computadores fora desta rede por meio de conexão remota;
- As estações de trabalho da rede Royal Magnífica possuem ferramenta para acesso remoto autorizado somente pela equipe de tecnologia. Podendo somente esta equipe acessar a estação com o aviso prévio ao usuário e para fins de manutenção ou suporte a sistemas e aplicações;
- O usuário não poderá remover ou bloquear programas de acesso remoto a estação;
- Os usuários da Royal Magnífica situados em ambientes externos poderão acessar sistemas internos somente por ferramentas homologas pela GEINF e por equipamentos de propriedade da empresa;
- Os acessos externos pelos usuários poderão acessar somente em horário de expediente;
- A conexão será validada mediante login e senha de rede do usuário;
- A ferramenta de acesso remoto deverá garantir o mínimo para a trilha de auditoria, sendo necessário solicitar e validar a identificação do usuário (login e senha), o horário de logon e logoff e histórico do que foi acessado;
- O acesso a sistemas interno somente será disponibilizado ao usuário quando for solicitado formalmente pelo gestor do usuário através do sistema de chamado e após ser analisado pela GEINF;
- A equipe de tecnologia da Royal Magnífica tem permissão para acesso remoto a estações de trabalho de usuários e a servidores;
- O acesso remoto só é permitido para o fim de manutenção e/ou suporte em sistemas e/ou aplicações;
- As ferramentas de acesso remoto deverão garantir o mínimo para a trilha de auditoria, sendo necessário solicitar e validar a identificação do usuário (login

e senha), identificar o horário de logon e logoff e histórico do que foi acessado;

- O gestor do usuário deverá solicitar a remoção do acesso quando este não fizer mais parte das suas obrigações;
- A GEINF é a área responsável pela disponibilização e manutenção dos acessos a ferramenta de conexão remota;
- A homologação de ferramenta para acesso remoto é de responsabilidade da GEINF.

INVENTÁRIO DOS ATIVOS

Objetivos:

Definir como deverão ser identificados e registrados os ativos da organização.

Diretrizes:

- Todos os ativos da Royal Magnífica são identificados com placas de identificação ou por seu número de série e documentados em inventário;
- O inventário deverá ser atualizado periodicamente;
- Os ativos inventariados deverão ter seu responsável indicado classificado.

USO ACEITÁVEL DOS ATIVOS

Objetivos:

Definir as regras para o uso dos ativos da organização sejam elas informações ou objetos.

Diretrizes:

- Todos usuários deverão ser conscientes dos requisitos de segurança da informação dos ativos da organização;
- Todos usuários são responsáveis pelo seu uso de qualquer recurso de processamento da informação e tal uso seja realizado sob sua responsabilidade;

DEVOLUÇÃO DOS ATIVOS

Objetivos:

Define que os ativos da organização emprestados para os colaboradores para a realização do seu trabalho deverão ser devolvidos a organização.

Diretrizes:

- Todos os funcionários ou prestadores de serviço devem devolver todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, contratos ou acordos;
- A não devolução ou a devolução parcial ou com dano no ativo acarretará penalidades previstas em lei;

DISPOSITIVOS MÓVEIS

Objetivos:

Define as medidas que apoiam a segurança da informação no gerenciamento de riscos decorrentes do uso de dispositivos móveis.

Diretrizes:

- Os dispositivos móveis pertencentes a empresa Royal Magnífica são todos cadastrados em sistema e associados a seus respectivos dados como IMEI, endereço MAC, marca, modelo e versão de sistema;
- Somente será disponibilizado ao usuário o dispositivo móvel após autorização do gestor usuário e do termo de responsabilidade de dispositivo móvel devidamente assinado por ele;
- A aquisição e instalação de sistemas de proteção física (capa, película, etc) dos dispositivos móveis são de inteira responsabilidade do usuário devendo ele adquirir e instalar no mais breve possível a fim proteger o exterior do equipamento;
- A versão do sistema operacional dos dispositivos não poderá ser alterada. As necessidades de atualização deverão ser comunicadas a área de telefonia e devidamente autorizada por ela;
- Os dispositivos móveis da empresa são cadastrados na rede wireless de acesso comum, não fazendo parte da rede interna da Royal Magnífica;
- Não é permitida a alteração do chip GSM disponibilizado pela empresa nem a sua substituição por outro chip GSM de linha pessoal;
- É proibido a utilização de conta particular como conta primária nos dispositivos da empresa;
- O usuário não poderá remover os softwares padrões da empresa Royal Magnífica;
- Os dispositivos deverão conter senha de acesso. Protegendo assim a confidencialidade dos dados da empresa;
- O back-up dos dados e da agenda telefônica é de inteira responsabilidade do usuário;
- O usuário é responsável pela segurança contra códigos maliciosos;
- É de inteira responsabilidade do usuário o uso correto do pacote de dados e minutos de ligações, não sendo possível a aquisição de dados excedentes e nem de minutos de ligação pela empresa nem pelo usuário;

- Quanto ao roubo, ao furto e a perda do dispositivo móvel, é de inteira responsabilidade do usuário a comunicação imediata à área de telefonia da empresa para que ações de segurança sejam tomadas;

E-MAIL

Objetivos:

Este regulamento define a forma de uso da ferramenta de correio eletrônico da organização, o que é proibido e a responsabilidade do usuário.

Diretrizes:

- É de responsabilidade da GEINF prover serviço de e-mail corporativo para funcionários e estagiários da empresa. Criar, bloquear e remover contas de e-mail e grupos de e-mail, e monitorar as atividades das contas;
- O serviço de correio eletrônico tem a finalidade única de comunicação institucional sendo restringido para:
    - Praticar crimes e infrações de qualquer natureza;
    - Ações nocivas contra recursos computacionais da Royal Magnífica ou de redes externas;
    - Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório ou de qualquer forma contrário a lei;
    - Disseminar vírus, spam, anúncios publicitários ou qualquer mensagem em forma de corrente;
    - Enviar informações sigilosas ou endereços de correio eletrônico corporativo;
- O usuário é o responsável pela manutenção da sua caixa de e-mail devendo ele eliminar aqueles e-mails que não são mais necessários, evitando que chegue a sua capacidade máxima;

- O acesso ao e-mail é restringido apenas ao ambiente interno da empresa, exceto em caso de função do usuário que necessite do acesso externo;
- O acesso ao serviço de e-mail se dará por login e senha de caráter pessoal e intransferível;
- Não é permitida a configuração de e-mail funcional em dispositivo móvel particular;
- É de responsabilidade do usuário todas as mensagens eletrônicas enviadas a partir de sua conta;
- A Royal Magnífica não se responsabiliza pelo back-up de e-mail;
- A utilização da foto de perfil em e-mail não é obrigatória, mas se usada, só poderá ser a foto do crachá disponível na intranet;
- As mensagens eletrônicas emitidas a partir do e-mail corporativo da Royal Magnífica devem conter, obrigatoriamente, assinatura, conforme descrito na instrução Correspondências que compõe o Manual de Normas e Instruções;
- A inclusão do e-mail do usuário a um grupo de e-mail deverá ser solicitada pelo gestor do grupo através do sistema de chamado;
- É proibido o usuário de fazer sua exclusão de qualquer grupo participante. Para isso, deverá ele ou o gestor do grupo solicitar pelo sistema de chamado essa ação;
- A comunicação externa através da conta de e-mail obedecerá às necessidades de cada gerência da empresa;
- As contas de usuários desligados da empresa serão suspensas no momento do seu desligamento;
- O back-up da conta de usuário suspenso poderá ser solicitado pelo gestor do usuário até 30 dias após seu desligamento da empresa após o tempo limite a conta será deletada da base de dados;
- A utilização irregular do recurso de e-mail poderá envolver em medida disciplinar administrativa e sansões previstas em lei.

INTERNET

Objetivos:

Dispor a forma como deverá ser acessada a internet pelos funcionários da Royal Magnífica.

Diretrizes:

- O uso da internet e da intranet deve ser usado para as atividades relacionadas ao negócio da empresa Royal Magnífica, de modo a contribuir com a produtividade do trabalho exercido;
- O acesso a internet deverá ser solicitado pelo gestor do usuário em sistema de chamado;
- O acesso à internet deverá ter níveis diferentes conforme a necessidade dos serviços e com perfis definidos pela GEINF;
- É permitido ao colaborador o uso da internet para fins particulares, desde que a utilização não impacte o seu desempenho e não ponha em risco a segurança da empresa;
- O usuário é totalmente responsável pelas ações e acessos realizados por meio da sua conta de acesso;
- O acesso a internet será validado perante login e senha da rede;
- Cabe a GEINF prover o recurso de internet para os usuários;
- Não é permitido o acesso a sites com conteúdo ofensivo, ilegal ou impróprio, como:
    - Conteúdo pornográfico, preconceituoso, de vandalismo, etc;
    - Download de programas e arquivos;
    - Site de Proxy anônimo;
    - Salas de bate-papo e jogos on-line;

- Compartilhamento de arquivos peer-to-peer (2P2);

- O usuário poderá solicitar o desbloqueio de páginas pelo sistema de chamado, que poderá ser desbloqueada ou não após a análise da GEINF;
- Todo acesso a internet será monitorado e mantido os logs de acesso;
- A utilização irregular do recurso de internet poderá envolver em medida disciplinar administrativa e a sansões previstas em lei;

INTRANET

Objetivos:

Dispor da forma como deverá ser utilizada o ambiente de comunicação interna via web da organização.

Diretrizes:

- A intranet é de uso comum aos usuários da empresa Royal Magnífica. Todos os colaboradores, estagiários e menores aprendendizes tem direito a acesso aos seus conteúdos;
- O acesso ao serviço de intranet deverá ser feito mediante login e senha pessoal e intransferível;
- A intranet deverá ser utilizada como mecanismo de divulgação de notícias e disponibilização de serviços de caráter institucional;
- O gerenciamento de conteúdo será feito por gerencia especifica, destinada à comunicação da empresa;

SEGURANÇA FÍSICA E DO AMBIENTE

Objetivos:

Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e as informações da organização.

Diretrizes:

- Para o acesso as partes internas pelo colaborador da Royal Magnífica é necessário o uso do crachá e de uniforme como meio de identificação;
- As portarias de acesso serão guardadas por vigilantes, recepcionistas e sistema de câmera de segurança;
- A entrada de visitantes a empresa somente será permitida após ser identificado na recepção e autorizado por um funcionário;
- A identificação do visitante se dará por meio de nome, CPF, RG, telefone;
- O acesso a sala de servidores de terceiros se dará somente por autorização e acompanhamento de funcionário do setor;
- A sala de servidores é protegida por meio de câmeras de segurança no padrão 24/7, equipamento termohígrografo, ar-condicionado, barreiras solidas, e por fechadura de liberação por senha pessoal e intransferível;
- O CPD e os switches deverão ser alimentados com redundância de energia para que sejam protegidos contra falta de energia elétrica;
- Deverão ser mantidos os logs de acessos a sala dos servidores em meio físico e/ou eletrônico;
- Os ambientes da Royal Magnífica serão monitorados 24/7hs por meio de circuito de câmeras de tvs e por alarme de detecção de intrusos;
- As salas de serviços deverão ser trancadas, as luzes apagadas e ar-condicionado desligado sempre quando não houver mais expediente;

MANUTENÇÃO EM EQUIPAMENTOS

Objetivos:

Estabelecer critérios para que sejam realizadas manutenções em equipamentos de forma a assegurar sua disponibilidade e integridade.

Diretrizes:

- Deverão ser feitos manutenções periódicas em equipamentos proprietários ou de terceiros em intervalos recomendados pelo fornecedor e de acordo com suas especificações;
- A manutenção deverá ser feita por pessoal especializado e devidamente autorizado;
- Deverão ser anotadas e guardadas todos os registros de falhas, suspeitas ou reais e o histórico de todas as manutenções realizadas em cada equipamento;
- Os equipamentos deverão ser testados após a sua manutenção antes de que seja disponibilizado novamente ao uso;

REMOÇÃO OU EMPRÉSTIMO DE ATIVO

Objetivos:

Disciplina que equipamentos, softwares, informações ou objetos não sejam retirados do local sem autorização prévia.

Diretrizes:

- Os gestores ou pessoas indicadas por eles deverão ser responsáveis pela permissão da remoção ou empréstimo de ativos para fora de setor ou da empresa;
- Deverão ser registrados as remoções ou empréstimos mantendo o mínimo de característica do ativo junto com sua identificação, dia da saída e data de retorno e nome do custodiante;
- Deverá ser assinado pelo solicitante termo de retirada de equipamento, software, informações ou objetos a fim de se responsabilizar pelos danos em sua posse;

SEGURANÇA CONTRA CÓDIGOS MALICIOSOS

Objetivos:

Estabelecer que ambiente de tecnologia seja protegido por ferramentas de detecção, prevenção e recuperação contra códigos maliciosos.

Diretrizes:

- A Royal Magnífica deverá dispor de ferramenta de proteção contra códigos maliciosos em todas estações de trabalho e servidores;
    - Esta ferramenta deverá realizar varreduras periodicamente em todos equipamentos;
- A ferramenta de proteção contra códigos maliciosos deverá estar atualizada constantemente;
- É proibido pelo usuário desinstalar ou manipular a ferramenta de proteção contra códigos maliciosos;
- A instalação de softwares não autorizados e não homologados pela GEINF é determinantemente proibida;

- Os acessos a sites externos deverão ser verificados pela ferramenta de proteção contra códigos maliciosos e deverão ser bloqueados se houver risco a organização;
- Deverá ser criado planos de continuidade do negócio para em caso de ataques por códigos maliciosos
- Os usuários com índice alto de incidência em detecção de vírus deverão ser comunicados formalmente pela gerência apropriada sobre os riscos iminentes;
- A GEINF é a área responsável por toda análise e manutenção das ferramentas de proteção contra códigos maliciosos, portanto, toda dúvida ou suporte deverá ser comunicada diretamente a ela.

CÓPIAS DE SEGURANÇA (BACK-UP)

Objetivos:

Definir os requisitos para às cópias de segurança das informações, dos softwares e dos sistemas, sua abrangência e frequência de gravação.

Diretrizes:

- As cópias de segurança deverão ser realizadas unicamente de documentos, softwares e sistemas críticos para a continuidade das operações da organização;
- São realizados dois tipos de cópias de segurança, uma completa e outra diferencial;
- Essas cópias deverão ser gravadas em mídias de longo prazo de vida útil e armazenadas em locais distantes do CPD, afim de que seja garantida a sua disponibilidade;

- As mídias de cópias de segurança deverão ser transportadas e guardadas por empresa especializada;
- Deverão ser realizados testes de restauração dos arquivos após sua conclusão de gravação para garantir a sua disponibilidade e integridade;
- A gerência responsável pela gestão das cópias de segurança fica a cargo da GEINF;
- As demandas de restauração de arquivos dispõem de até 72 horas para que sejam concluídas;
- As cópias de segurança são armazenadas num período máximo de cinco anos, a contar da data de aniversário;

REGISTROS E MONITORAMENTO

Objetivos:

Definir que registros (logs) de atividades de sistemas e de usuários deverão ser implementados e sistemas de monitoramento

Diretrizes:

- Os sistemas da Royal Magnífica deverão gerar e armazenar os logs de eventos das atividades dos usuários, exceções, falhas e eventos de segurança por um tempo mínimo de dois anos;
- Os relógios de todos os sistemas de processamento de informações deverão ser sincronizados com uma única fonte de tempo dentro do domínio da organização;
- Os logs de acesso dos usuários deverão conter o mínimo de informação como a identificação do usuário, atividade realizada, arquivos acessados, a data e a hora de logon e logoff e de alteração de dados e o tipo de ação realizada no acesso.

RESTRIÇÕES DE INSTALAÇÕES DE SOFTWARE

Objetivos:

Definir os critérios para instalação de software nos computadores da organização;

Diretrizes:

- As instalações, atualizações ou mudanças de software deverão ser realizadas somente pela área de suporte técnico da organização;
- Controles de configuração e de versão deverão ser implementados para que se obtenha o controle de implementação de softwares;
- Versões anteriores dos softwares deverão ser mantidas com medida de contingência;
- As instalações de software poderão ser feitas de forma automatizada pela área de suporte;
- Somente softwares homologados e licenciados pela área técnica e de cunho profissional poderão ser utilizados na organização;
- A utilização de sistemas, programas e software de propriedade da Royal Magnífica só poderão ser utilizados para desenvolvimento de trabalhos profissionais para a organização;
- É proibida a cópia de softwares em quaisquer tipos de mídias e de suas licenças adquiridas pela Royal Magnífica;
- A área de tecnologia deverá ter a lista de todos os softwares e suas licenças guardadas e atualizadas.

DA AUDITORIA

Objetivos:

Definir o método para que seja realizada as auditorias com o mínimo de impacto e interrupções dos processos do negócio.

Diretrizes:

- Os acessos aos sistemas e dados pela auditoria deverão ser acordados com o gestor da informação;
- O processo de auditoria será sempre autorizado de maneira formal pela Presidência da organização;
- Os acessos de auditoria deverão ser limitados somente a leitura de dados;
- Os acessos diferentes as leituras deverão ser permitidas apenas em cópias isoladas dos dados;
- Todo o acesso aos dados e sistemas deverão ser monitorados e registrados para que seja produzida uma trilha de acessos;
- Cabe a DITEC fornecer os meios, processos e recursos para o desempenho das atividades de auditoria.

DA CLASSIFICAÇÃO DA INFORMAÇÃO

Objetivos:

Definir que a informação receba um nível adequado de proteção de acordo com sua importância.

Diretrizes:

- A classificação e controles de proteção para a informação deverão ser implementados levando em consideração as necessidades do negócio da organização;
- Os proprietários de ativos de informação deverão ser os responsáveis por sua classificação;
- A classificação da informação será feita de acordo com a sua confidencialidade, integridade e disponibilidade;
- A classificação se dará das seguintes formas:
    - Confidencial: informação de divulgação mais restrita e sensível a organização;
    - Interno: informação restritas aos colaboradores e prestadores de serviço da organização;
    - Público: informação liberada para o público em geral - clientes, fornecedores e estagiários;

CONSCIENTIZAÇÃO, EDUCAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

Objetivos:

Definir que treinamentos, educação e conscientização em segurança da informação e a comunicação da política de segurança e suas atualizações sejam realizadas a todos funcionários da organização.

Diretrizes:

- A organização deverá fornecer programa de conscientização, treinamento e educação em segurança da informação a todos seus colaboradores;
- A organização deverá comunicar a todos colaboradores, da forma que achar mais adequada, as atualizações da sua Política de Segurança da Informação;

- O programa de conscientização deverá participar do calendário institucional como objetivos para a organização e realizado periodicamente;
- O programa de conscientização deverá ser atualizado regularmente para que permaneça alinhado com as políticas e procedimentos da organização e com base nas lições aprendidas dos incidentes da informação;
- Os programas de conscientização em segurança da informação deverão ser declarados como o comprometimento da direção com a segurança da informação em toda a organização;

ANEXO A – PROPOSTA DE CAMPANHA SENHAS

Proposta: Campanha Sua Senha, Nossa Segurança.

Gerência de Comunicação Interna – GECOI

I) Apresentação

A Gerência de Tecnologia - GETEC tendo por objetivo aperfeiçoar continuadamente a Gestão de Segurança da Informação da Royal Magnífica considera importante realizar uma campanha de conscientização dos colaboradores da Empresa. Quanto à responsabilidade do exercício da função de Usuário dos Sistemas Computacionais.

O aperfeiçoamento constante dos recursos tecnológicos visando proteger os dados tem esbarrado em um problema recorrente: a pouca percepção, por parte do colaborador, quanto a sua corresponsabilidade pela segurança das informações, conforme estabelece a Norma ABNT NBR ISO/IEC 27001:2013.

Tornar efetivas as práticas de proteção e renovação periódica das senhas dos usuários contribui para a eficácia das medidas de proteção dos Sistemas.

II) Objetivos

a) Conscientizar os colaboradores de sua responsabilidade formal pela segurança da informação.

b) Difundir as boas práticas de segurança em relação ao uso e proteção da senha de acesso.

III) Nome da campanha

Sua Senha, Nossa Segurança.

IV) Ícone da campanha

Uma chave estilizada com a frase “Sua Senha, Nossa Segurança”.

V) Slogan

Proteger a Senha é responsabilidade do Colaborador!

VI) Público-alvo

Colaboradores da Empresa Royal Magnífica.

VII) Metodologia para a campanha

a) Primeira etapa: sensibilizar os colaboradores para a responsabilidade formal enquanto Usuário dos Sistemas Royal, relativamente à segurança da informação, em conformidade com a política de sigilo.

b) Segunda etapa: informar e reiterar os procedimentos de proteção à senha e sua atualização periódica.

VIII) Estratégia de divulgação

a) **1º momento:** lançamento da campanha.

b) **2º momento:** Informes sobre a responsabilidade do Usuário.

c) **3º momento:** Informes sobre melhores práticas de segurança.

d) **4º momento:** Lembretes mensais de reforço.

IX) Peças a serem produzidas

a) Identidade visual.

b) Informes.

X) Áreas envolvidas

a) GETEC.

b) GECIN.

XI) Cronograma de produção de peças

ETAPAS	**PRAZOS**
Briefing	Outubro
Criação	de 19/10 a 25/11
Apresentação	26/11
Aprovação	até 1º/12
Período da divulgação	de 02/02/2016 a 10/03/2016

XII) Cronograma de divulgação

DATA	**PEÇA**	**PARA**
02/02/16	Informe de Lançamento	Funcionarios@
15/02/16	Informe Educativo 1	Funcionarios@

17/02/16	Informe Educativo 2	Funcionarios@
25/02/16	Informe Educativo 3	Funcionarios@
29/02/16	Informe Melhores Práticas 1	Funcionarios@
04/03/16	Informe Melhores Práticas 2	Funcionarios@
08/03/16	Informe Melhores Práticas 3	Funcionarios@
10/03/16	Informe Melhores Práticas 4	Funcionarios@
Março a Dez/16	Lembretes Mensais	Funcionarios@

Brasília, 25 de novembro de 2015.

Atenciosamente,

Alicia Lins

Gerente Executiva

Tel.: (61) 3555 9999 Fax.: (61) 3555 9988

ANEXO B – ANTIGA POLÍTICA DE SEGURANÇA

14.3. Segurança da Informação

A presente instrução tem a finalidade de estabelecer as diretrizes para a utilização dos recursos de tecnologia da informação nas Empresa Royal Magnífica.

14.3.1. Das definições

a) Administradores: pessoas ou equipe com delegação do superior hierárquico para administrar um determinado ambiente informatizado.

b) Firewall: “um software ou um hardware que verifica informações provenientes da Internet ou de uma rede e as bloqueia ou permite que elas cheguem ao computador, dependendo de suas configurações”.

c) Proxy: “computador que funciona como intermediário entre um navegador da Web (como o Internet Explorer) e a Internet. Os servidores proxy ajudam a melhorar o desempenho na Web armazenando uma cópia das páginas da Web utilizadas com mais frequência. Também contribuem para a segurança porque filtram alguns tipos de conteúdo da Web e softwares mal-intencionados”.

d) Servidores: equipamentos que servem como repositório de dados ou gerenciam recursos da rede, de acordo com os padrões tecnológicos estabelecidos pela Royal Magnífica.

e) Usuários: pessoas que utilizam os recursos de tecnologia da informação de propriedade ou controlados pela Royal Magnífica (colaboradores, prestadores de serviços, clientes e fornecedores).

f) Recursos críticos: equipamentos e/ou serviços imprescindíveis à continuidade dos negócios da Royal Magnífica.

14.3.2. Dos objetivos

a) Garantir a proteção das informações referentes às Empresa Royal Magnífica, de seus clientes, de seus parceiros e fornecedores.

b) Assegurar o cumprimento legal no que tange a pirataria, licenciamento, direitos autorais e plágio.

c) Estabelecer as condições adequadas para a utilização dos recursos de tecnologia da informação pelos colaboradores e pelos prestadores de serviços das Empresa Royal Magnífica.

14.3.3. Da aplicação

A presente instrução aplicar-se-á a todas as Empresa Royal Magnífica.

14.3.4. Dos agentes responsáveis

a) Todos são responsáveis pelo uso que fazem dos recursos de tecnologia da informação, como também pela integridade dos equipamentos utilizados e pela confidencialidade das informações a que têm acesso em função do cargo que ocupam nas Empresa Royal Magnífica.

b) Cada usuário é responsável pelas informações armazenadas e/ou acessadas utilizando-se os equipamentos sob sua responsabilidade. No caso de equipamentos de utilização coletiva, essa responsabilidade será do principal gestor da área.

c) Os Diretores, Superintendentes, Chefes de Departamento, Gerentes Executivos e principais gestores são responsáveis pelo cumprimento das orientações referentes à segurança da informação pelos colaboradores sob sua responsabilidade.

d) A Diretoria de Tecnologia – DITEC é responsável por coordenar a administração e a manutenção dos sistemas informatizados (novos ou já implantados) e dos recursos de tecnologia da informação utilizados nas Empresa Royal Magnífica; por autorizar a conexão de equipamento de tecnologia de terceiros à rede da Royal Magnífica; e também pela prática dos atos descritos em suas atribuições e alçadas.

e) A Gerência de Desenvolvimento de Sistemas – GEDEN é responsável pelo gerenciamento e monitoramento de todas as atividades relacionadas às áreas de desenvolvimento de sistemas, de Internet/Intranet, de administração de bancos de dados e ainda pela prática dos atos descritos em suas atribuições e alçadas.

f) A Gerência de Suporte Tecnológico – GESUP é responsável pelo gerenciamento e monitoramento das atividades relacionadas à rede de dados, a telecomunicações, a acessos à Internet e à utilização de e-mail corporativo e dos equipamentos de tecnologia da informação, como também pela prática dos atos descritos em suas atribuições e alçadas.

14.3.5. Das disposições gerais

a) As informações acerca das Empresa Royal Magnífica são ativos que exigem proteção especial.

b) Os recursos de telecomunicações, equipamentos e serviços de tecnologia da informação são propriedade da Empresa, fornecidos como ferramentas para permitir que os colaboradores desempenhem suas atividades.

c) Ao utilizarem recursos tecnológicos, todos os colaboradores devem atuar em conformidade com as regras legais pertinentes à moral, à integridade e aos bons costumes, tendo comportamento compatível com o Código de Ética da Royal Magnífica.

d) Somente pessoas autorizadas pelo principal gestor da área devem utilizar os recursos de tecnologia da informação fornecidos pela Royal Magnífica, sendo seu uso limitado exclusivamente aos usuários da Empresa.

e) Fica proibida a exploração de falhas ou vulnerabilidades porventura existentes nos sistemas. Quando detectadas, essas devem ser comunicadas imediatamente à GEDEN.

f) Todas as tentativas de acesso ilegal aos sistemas de informação da Royal Magnífica, quando detectadas, serão passíveis de exame sob o aspecto disciplinar.

14.3.6. Do controle de acesso

a) Os sistemas informatizados devem ser acessados exclusivamente para a condução dos negócios das Empresa Royal Magnífica, exceto por autorização formal do superior hierárquico.

b) Devem ser respeitadas e cumpridas as normas de segurança e as restrições de sistema impostas pela Royal Magnífica, tais como direitos de acesso a arquivos, diretórios e recursos disponíveis no ambiente profissional, etc.

c) Os atos e acessos do usuário aos dados e sistemas da Royal Magnífica devem ser realizados por meio de sua identificação no ambiente empresarial (login e senha).

d) O acesso de usuários temporários ao ambiente informatizado da Royal Magnífica deve ser solicitado à GESUP, especificando-se o prazo durante o qual o usuário fará o acesso.

e) O RH deverá informar à GEINF sobre o período de férias ou licenças médicas de colaboradores (exceto do Presidente, dos Diretores, dos Superintendentes, dos Chefes de Departamento e dos Gerentes Executivos) para que os acessos desses usuários sejam bloqueados.

f) Cada usuário é responsável pela utilização das senhas corporativas necessárias ao desempenho de suas funções.

g) O principal gestor da área deve solicitar à DITEC – por escrito ou pelo e-mail atendimento@royalmagnifica.com.br – a inclusão, a exclusão e o bloqueio (alteração) de acesso e uso para usuários sob sua supervisão.

h) Quando da inclusão, os usuários recebem o acesso mínimo necessário para o desempenho de suas funções, salvo os casos em que o principal gestor solicitar formalmente outros níveis de acesso aos usuários de acordo com as necessidades de suas funções e atribuições profissionais.

i) A senha é de uso pessoal e intransferível, sendo proibido o seu compartilhamento. Caso isso ocorra, é de total responsabilidade do usuário proceder à sua alteração.

j) A senha de acesso deve conter, no mínimo, sete caracteres alfanuméricos (números e letras), sendo o usuário obrigado a escolher uma nova senha no momento do primeiro acesso.

k) Não é permitido o uso de senhas óbvias, como datas, nomes próprios e siglas. Ela deve ser memorizada e nunca anotada em lugar de fácil acesso aos outros usuários.

l) O usuário tem direito a cinco tentativas de autenticação de senha. Após a quinta tentativa frustrada, seu acesso será bloqueado até a posterior autorização de liberação pela GESUP/GEINF.

m) A senha possui validade de 90 dias. Ao término desse período, será automaticamente
solicitada a sua troca.

n) Para efeito de histórico, são armazenadas as sete últimas senhas utilizadas, não sendo permitido o seu uso para a gravação de uma nova senha.

o) Caso a GESUP suspeite de perda de sigilo da senha de um usuário, esse terá o acesso bloqueado e o principal gestor da área será avisado quanto ao ocorrido.

14.3.6.1. Do acesso remoto

a) A DITEC deve garantir as medidas de segurança necessárias para o correto acesso remoto a canais de comunicação externos, tais como modens, gravadores de mídias (CDRW, DVDR, Floppy 3 ½) e portas USB (pendrive, máquinas fotográficas, gravadores de áudio e vídeo, etc.).

b) Desde dois de janeiro de 2014, as portas USB dos equipamentos eletrônicos das Empresas Royal Magnífica estão bloqueadas, a fim de minimizar as ocorrências de contaminação dos computadores por vírus.

c) Eventuais exceções à regra descrita na alínea “b” deste item são analisadas caso a caso, mediante solicitação formal do respectivo Diretor da área para o e-mail atendimento@royalmagnifica.com.br.

14.3.6.2. Do acesso físico

Os colaboradores que desempenham atividades de apoio ou de serviços gerais devem acessar a Sala dos Servidores somente em horário pré-determinado pelo responsável pela área, sendo, inclusive, acompanhados por um profissional do quadro de colaboradores da GESUP para a execução de suas tarefas nesses locais.

14.3.7. Do uso de software

a) A utilização de sistemas, de programas, de aplicativos e de softwares em geral deve estar restrita aos funcionários autorizados e homologados pela Royal Magnífica.

b) A DITEC deve possuir a lista dos softwares autorizados para uso na Royal Magnífica, sendo de responsabilidade de cada setor o envio periódico à DITEC da relação atualizada dos softwares utilizados no local.

c) É proibida a cópia de softwares adquiridos ou desenvolvidos pela Royal Magnífica para uso na residência de seu contingente de colaboradores, bem como de prestadores de serviços terceirizados contratados pela Empresa. Autorização especial poderá ser concedida, desde que com o consentimento prévio da DITEC.

d) Não é permitido o uso de softwares que não tenham sido homologados, licenciados e adquiridos mediante processo legítimo de compra pela Royal Magnífica.

e) O usuário será responsabilizado pelo uso de software não autorizado de acordo com o estabelecido no item

14.3.29. Das penalidades.

No caso de estações compartilhadas, o principal gestor da área será responsabilizado.

f) Não é permitida a cópia/reprodução de nenhuma mídia que não tenha sido produzida ou adquirida pela Royal Magnífica.

14.3.8. Do uso de hardware

a) É permitida a conexão na rede Royal Magnífica apenas de equipamentos autorizados pela Empresa.

b) Compete à DITEC, em conjunto com as demais áreas que compõem a Royal Magnífica, estabelecer um padrão mínimo dos equipamentos da Empresa.

c) Os notebooks devem ser acondicionados e transportados em mochilas apropriadas, com identificação visível e não removível. É obrigatória a assinatura, pelo usuário, de um termo de responsabilidade que estabelece os direitos e os deveres quanto utilização, posse e guarda do equipamento e das informações nele armazenadas.

d) Os equipamentos de terceiros (aluguel, empréstimo, particulares, etc.) possuem identificação específica que os diferencia daqueles utilizados pela Royal Magnífica. No entanto, esses equipamentos são, da mesma forma, controlados pela Empresa.

e) O manuseio dos equipamentos deve preservar sua integridade física e seu bom funcionamento, bem como estar em conformidade com as recomendações de conservação e uso fornecidas pelo fabricante.

14.3.9. Do uso dos dispositivos de Web utilizados pela Royal Magnífica

a) O uso da Internet, da Intranet e do e-mail corporativo deve restringir-se às atividades relacionadas aos negócios da Royal Magnífica, de modo a contribuir para a produtividade do trabalho exercido na Empresa.

b) É permitido ao colaborador o uso desses recursos para fins particulares, desde que sua utilização não prejudique o desempenho do funcionário na função para a qual foi contratado; que não exponha a Empresa a riscos legais ou ao vazamento de informações estratégicas e sigilosas; e que sejam observadas as regras judiciais vigentes.

c) Não é permitida a utilização da Internet e do e-mail corporativo para acessos não autorizados a computadores, redes, bancos de dados ou a informações armazenadas eletronicamente.

d) Não é facultado ao colaborador o direito à privacidade de informações obtidas por meio dos recursos de tecnologia da informação utilizados na Royal Magnífica.

e) Não é permitido o acesso a sites de conteúdo ofensivo ou inadequado ao ambiente de trabalho, bem como a troca de mensagens eletrônicas com declarações ofensivas, de cunho sexual ou inapropriadas ao desempenho das funções dentro das Empresa Royal Magnífica.

14.3.9.1. Do uso da Internet e da Intranet da Royal Magnífica

a) A Internet e a Intranet são consideradas aplicações críticas. Dessa forma, o seu uso está condicionado à solicitação formal do principal gestor da área aos setores responsáveis.

b) É proibido o uso de meios de conexão com a Internet e outras redes que não sejam os fornecidos pela Empresa.

c) O uso interno da Internet e da Intranet é permitido via firewall e proxy da Royal Magnífica.

d) As atividades relacionadas à Intranet (Index Royal Magnífica) são gerenciadas pela Gerência de Comunicação Interna – GECOI, mediante prévia articulação com a DITEC.

e) Não é permitida a realização de download de programas e/ou de softwares não autorizados nos equipamentos da Royal Magnífica.

f) O acesso à Internet será monitorado por meio de software especialista, sendo o relatório de controle enviado às áreas responsáveis desde que mediante solicitação formal do principal gestor do setor.

g) A divulgação de vídeos/filmes publicitários, fora do ambiente da Intranet (Index Royal Magnífica) deve ser feita mediante prévia consulta à DITEC, à Superintendência de Marketing e Publicidade – SUMAP ou à GECOI.

14.3.9.2. Do uso do e-mail corporativo

a) Desde 6 de maio de 2013, a Royal Magnífica utiliza a ferramenta de e-mail do pacote Google Apps For Business.

b) São de responsabilidade dos usuários todas as mensagens eletrônicas enviadas a partir de sua conta de correio eletrônico.

c) É terminantemente proibido o envio de mensagens do tipo correntes e spam pelo e-mail da Royal Magnífica.

d) O usuário deve remover do correio eletrônico mensagens obsoletas e não pertinentes às atividades despenhadas por ele na Royal Magnífica.

e) É facultativa a inserção da imagem do colaborador no e-mail corporativo. No entanto, os colaboradores que optarem pela sua inclusão devem fazê-lo, utilizando,

obrigatoriamente, a imagem do crachá, disponível na Intranet da Royal Magnífica no perfil de cada funcionário.

f) As mensagens eletrônicas emitidas a partir do e-mail corporativo da Royal Magnífica devem conter, obrigatoriamente, assinatura, conforme descrito na instrução Correspondências, que compõe o Manual de Normas e Instruções.

14.3.10. Da configuração das estações de trabalho e dos aplicativos

a) Fica proibida a alteração da configuração (hardware e software) das estações de trabalho existentes nas Empresa Royal Magnífica.

b) As estações de trabalho devem possuir software padrão para combate a vírus eletrônico, configurado e ativado, não podendo ser desativado pelo usuário em hipótese alguma.

c) O usuário deve informar à DITEC, por meio do endereço eletrônico atendimento@royalmagnifica.com.br, quaisquer suspeitas de contaminações na sua estação de trabalho por vírus eletrônico.

d) A ocorrência de problemas deve ser registrada pelo usuário, que deve solicitar a abertura de um chamado pelo endereço eletrônico tendimento@royalmagnifica.com.br ou pelo ramal 7095 (somente para os casos em que não haja a possibilidade de acionamento do setor pelo e-mail indicado).

14.3.11. Do comportamento esperado dos usuários

a) Manter a necessária cautela quando da exibição de dados em tela e em impressora ou da gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas.

b) Encerrar/bloquear a sessão de uso do sistema sempre que se ausentar da estação de trabalho, garantindo, assim, a impossibilidade de acesso indevido por pessoas não autorizadas.

c) Zelar pela integridade, pela confidencialidade e pela disponibilidade das informações contidas nos sistemas.

d) Comunicar, por escrito, à chefia imediata quaisquer indícios ou possibilidades de irregularidades, desvios ou falhas identificadas nos sistemas.

e) Reportar imediatamente ao superior hierárquico toda situação que não esteja prevista nesta norma e que possa comprometer a integridade e a segurança das informações, bem como dos recursos fornecidos pela Royal Magnífica.

14.3.12. Do armazenamento de arquivos

a) As informações restritas ou confidenciais atinentes à Royal Magnífica devem ser armazenadas em diretório próprio na rede da Empresa, não devendo ser guardadas fora desse ambiente.

b) Os colaboradores não devem armazenar documentos particulares nos servidores da Royal Magnífica. Esses arquivos serão excluídos sem prévio aviso sempre que for constatada a sua existência.

C) Será permitida a guarda de arquivos particulares nos desktops, notebooks e demais recursos fornecidos pela Empresa, desde que esses não provoquem risco legal para a Royal Magnífica e não prejudiquem a utilização do equipamento.

d) Em caso de dúvida, os colaboradores devem procurar orientação com seus gestores, a fim de saber como proceder.

e) A Royal Magnífica não se responsabiliza por conteúdo, manutenção, backup, cópia ou recuperação de arquivos particulares.

f) Não será permitido o uso de dispositivos pessoais nos equipamentos e recursos da Empresa. A Royal Magnífica fornecerá os recursos necessários para o desempenho de cada função.

14.3.13. Do backup de arquivos

a) São realizados os seguintes tipos de backup:

I. de rede: realizado diariamente em todos os servidores sob a responsabilidade da DITEC;
II. de banco de dados: realizado diariamente nos servidores de banco de dados sob a responsabilidade da DITEC.

b) Cabe à DITEC, em conjunto com as demais gerências responsáveis, estabelecer a política, a periodicidade e o tempo de retenção das mídias na execução de backups.

c) A GESUP é responsável pela execução de backups e deve estabelecer um prazo para Revisão periódica, a fim de testar a restauração e a integridade dos backups.

d) A guarda das fitas de backup é feita por uma empresa especializada.

14.3.14. Da manutenção, da administração e da segurança dos recursos de tecnologia da informação

a) Os administradores de sistemas existentes em cada área da Royal Magnífica devem ter substitutos capacitados para desenvolver suas atividades em suas ausências.

b) Cabe à DITEC elaborar e manter a documentação lógica dos sistemas de informação da Royal Magnífica sempre atualizada e disponível para auditoria.

c) A DITEC deve, obrigatoriamente, proceder à análise do impacto na segurança em função da adoção de novas tecnologias e normas.

d) A administração da rede e sistemas deve ser realizada com o auxílio de ferramentas de segurança ou procedimentos adequados para tal finalidade.

e) Não é permitido o acesso aos recursos de tecnologia da informação da Royal Magnífica por meios não autorizados pela Empresa.

f) A disponibilidade ininterrupta de recursos críticos deve estar assegurada pela existência de cópia de segurança e de plano de contingência.

g) Os links considerados críticos devem possuir opção de contingência.

h) A DITEC deve desenvolver regras e mecanismos para garantir a efetividade, a continuidade e a segurança adequadas dos recursos de tecnologia da informação.

i) Todo recurso a ser disponibilizado em produção deve ser previamente controlado e homologado em ambiente de teste da DITEC.

j) As ferramentas de segurança devem ser configuradas a partir de procedimentos definidos pela DITEC.

k) Os softwares e os hardwares devem ser protegidos por ferramentas de segurança ou procedimentos que garantam o uso somente após identificação e validação do usuário, sendo bloqueadas em caso de tentativa de acesso não autorizada.

l) A DITEC deve desenvolver rotinas de manutenção preventiva para os equipamentos de acordo com seu tipo/porte, bem como com as normas estabelecidas pelos fabricantes.

14.3.15. Da auditoria

a) Cabe às Diretorias, ao Departamento de Auditoria Interna – AUDIT e à Assessoria Jurídica – AJURI solicitarem, caso necessário, a realização de auditoria nos equipamentos e/ou softwares utilizados pelo contingente de colaboradores das Empresa Royal Magnífica.

b) A atividade de auditoria será realizada sempre mediante autorização formal da Presidência da Royal Magnífica.

c) Cabe à DITEC prover meios, processos e recursos para o acompanhamento formal dos registros de acesso e a utilização dos recursos tecnológicos fornecidos pela Royal Magnífica nas aplicações onde os logs de auditoria estiverem habilitados.

d) Para efeito de auditoria e controle, devem ser registrados o início e o término do acesso, inclusive remoto, ao banco de dados, à Internet e aos sistemas.

e) Os registros de que trata o item anterior devem conter, no mínimo, as seguintes informações: usuário, data e hora do logon e do logoff.

14.3.16. Do combate a vírus

a) Cabe à DITEC possuir sempre a versão mais recente do software de antivírus, bem como definir um padrão de software de antivírus e elaborar os procedimentos para o caso de ocorrência de contaminação da rede da Royal Magnífica por vírus eletrônico.

b) Todo arquivo recebido, via Internet ou não, deve ser verificado pelo usuário antes de ser aberto ou executado, a fim de detectar a existência de vírus eletrônico. Na dúvida, o arquivo deverá ser encaminhado para atendimento@royalmagnifica.com.br, para análise.

14.3.17. Do lixo informático

a) Os administradores da GESUP devem monitorar a disponibilidade de espaço nos servidores, notificando, no caso de excesso de conteúdo, os principais gestores das áreas, a fim de que estes providenciem a remoção do lixo informático.

b) As informações inativas devem ser armazenadas, de maneira segura, fora do ambiente de produção, conforme a solicitação do principal gestor da área.

c) Os arquivos de músicas, de fotos e de vídeos de natureza particular não devem ser salvos na rede. Quando identificados pela DITEC, esses documentos serão apagados sem prévio aviso ou possibilidade de retorno, exceto aqueles estritamente necessários para o desenvolvimento das atividades na Royal Magnífica e desde que mediante justificativa formal do principal gestor da área.

14.3.18. Dos direitos autorais e plágio

Não é permitido o uso de equipamentos e recursos fornecidos pela Royal Magnífica para prática de pirataria de softwares, músicas, livros ou qualquer propriedade intelectual, seja para uso próprio ou de terceiros.

14.3.19. Da propriedade intelectual

Os colaboradores devem proteger e salvaguardar ideias, programas, planos e projetos concebidos pela Royal Magnífica, desenvolvidos por si próprios ou por terceiros contratados para esse fim.

14.3.20. Da publicação de informações

a) Fica proibida a divulgação de informações, confidenciais ou não, em nome ou a respeito da Royal Magnífica, em mídias sociais, blogs e demais meios de comunicação sem a prévia autorização da SUMAP.

b) Será responsabilizado o colaborador promotor de ações que provoquem danos à Empresa e/ou a terceiros, utilizando ou não os recursos de tecnologia da informação disponibilizados pela Royal Magnífica.

c) Fica proibida a utilização de logotipos ou marcas das Empresa Royal Magnífica em sites, em comunidades ou em outros materiais de divulgação sem a autorização da SUMAP e/ou da GECOI.

14.3.21. Do sigilo de informações estratégicas

a) Fatos ou informações de quaisquer naturezas obtidos no ambiente profissional não devem, em hipótese alguma, ser revelados fora desse ambiente, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autorização formal do superior hierárquico.

b) As informações sigilosas da Royal Magnífica devem ser armazenadas e/ou transferidas por meio da rede da Empresa, em diretórios específicos para cada finalidade, utilizando-se recursos de segurança.

c) Os diretórios (pastas) de trabalho devem ser compartilhados somente mediante atribuição de senha de acesso para essa finalidade e autorização formal do principal gestor da área.

d) Os funcionários que possuem acesso a informações sigilosas devem assinar o Termo de Compromisso, Sigilo e Confidencialidade (Anexo A).

14.3.22. Dos incidentes e/ou falhas de segurança

a) Os incidentes e/ou falhas no esquema de segurança da informação devem ser comunicados imediatamente à DITEC, que procederá ao registro para análise posterior.

b) A DITEC deve elaborar procedimentos de trabalho específicos para o registro dos casos de incidentes e/ou de violações de segurança.

14.3.23. Do plano de contingência

a) No caso de necessidade, o principal gestor da área definirá, com a DITEC, os procedimentos para a recuperação dos recursos de tecnologia da informação.

b) O plano de contingência deve ser testado e reavaliado periodicamente.

c) Nos ambientes computacionais, a chave de acesso de administrador deve ser armazenada pelo principal gestor da área, em local restrito e com controle de acesso.

d) Todos os processos de contingência relacionados à tecnologia da informação devem estar formalmente documentados pela DITEC e ser previamente aprovados

pelas respectivas Diretorias da Royal Magnífica, a fim de garantir o pronto restabelecimento desses ambientes em situações específicas.

14.3.24. Do atendimento ao usuário

a) Quando em atendimento, o técnico de suporte deve estar acompanhado pelo usuário, a fim de que seja mantida a proteção das informações e dos recursos.

b) O serviço prestado pelo técnico de suporte deve ser homologado pelo usuário.

14.3.25. Do desenvolvimento de sistemas

O processo de desenvolvimento de sistemas ou rotinas de informação deve seguir as seguintes diretrizes:

a) criação e atualização da documentação do sistema, bem como seu armazenamento em local seguro e controlado;

b) detalhamento dos requerimentos de segurança aos quais os sistemas devem atender obrigatoriamente;

c) utilização de trilhas de auditoria nas transações de negócio efetuadas pelos usuários e nos acessos aos códigos-fonte, no caso de sistemas/aplicações desenvolvidas com trilhas de auditoria.

d) uso de criptografia de senhas;

e) utilização de interfaces automatizadas entre sistemas, objetivando evitar transações incorretas;

f) segregação de funções;

g) não permissão ao acesso de usuários diretamente ao banco de dados de produção (versão em uso);

h) controle dos acessos aos códigos-fonte, visando evitar versões fraudulentas.

14.3.26. Da revisão da segurança

a) Cabe à DITEC revisar e verificar, periodicamente, a efetividade de todo documento que compõe esta instrução, buscando garantir que as práticas adotadas sejam adequadas e eficientes.

b) Todas as áreas devem ser submetidas, pela DITEC, a revisões regulares para constatar a conformidade com esta instrução.

14.3.27. Da classificação da informação

a) Para uma efetiva classificação da informação, devem ser consideradas as necessidades de compartilhar e/ou restringir o acesso à informação, bem como o seu uso, assim como os impactos relacionados a essas necessidades. Para tanto, deve ser utilizado o software de Gerenciamento Eletrônico de Documentos – GED, que fornece as garantias necessárias descritas nos artigos abaixo.

b) A classificação da informação define o conjunto apropriado de níveis de proteção, indicando a necessidade de medidas para a manipulação especial.

c) A classificação da informação segue níveis de sensibilidade e criticidade, conforme abaixo:

I. uso confidencial: informações cuja divulgação deve ser restrita e controlada. Sua liberação indevida pode causar grandes danos à Royal Magnífica;

II. uso interno: informações restritas aos colaboradores e aos prestadores de serviços da Royal Magnífica;

III. uso público: informações para o público em geral, incluindo clientes, fornecedores, estagiários, bolsistas, etc.

d) As normas de classificação da informação são aplicadas na Royal Magnífica. No entanto, os documentos recebidos de outras empresas podem apresentar regras de segurança diferentes.

14.3.28. Das infrações

a) Ressalvadas as hipóteses de requisições legalmente autorizadas, constituirá infração funcional e penal a revelação de segredos do negócio obtidos em razão do cargo.

b) Constituirá descumprimento de normas legais e regulamentares, além de quebra de sigilo funcional, divulgar para outros servidores ou pessoas não envolvidas nos trabalhos executados os dados obtidos nos sistemas aos quais se tenha acesso, estando sujeito o colaborador às penalidades previstas em lei e regulamentos internos.

c) Caracterizará infração funcional e penal inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos dos sistemas ou bancos de dados das Empresas Royal Magnífica, com a finalidade de obter vantagem indevida para si ou para outrem ou de causar dano, modificar ou alterar o sistema de informação ou programa de informática sem autorização e/ou solicitação de autoridade competente.

14.3.29. Das penalidades

O colaborador que infringir uma ou mais normas descritas anteriormente responderá disciplinar, penal e civilmente pelas consequências das ações ou das omissões de sua parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de sua senha ou das transações a que tenha acesso.